

AD-A229 625

UNITED STATES COPYRIGHT LAW  
AND SOFTWARE PIRACY ON  
UNITED STATES AIR FORCE  
MICROCOMPUTERS

THESIS

Jay C. Sorensen  
First Lieutenant, USAF

②

AFIT/GIR/LSY/90D-11



UNITED STATES COPYRIGHT LAW  
AND SOFTWARE PIRACY ON  
UNITED STATES AIR FORCE  
MICROCOMPUTERS

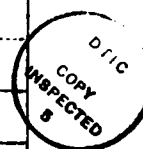
THESIS

Jay C. Sorensen  
First Lieutenant, USAF

AFIT/GIR/LSY/90D-11

The opinions and conclusions in this paper are those of the author and are not intended to represent the official position of the DOD, USAF, or any other government agency.

Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DWIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution	
Availability Codes	
Dist	Available d/or Special
A-1	



AFIT/GIR/LSY/90D-11

UNITED STATES COPYRIGHT LAW AND SOFTWARE PIRACY  
ON UNITED STATES AIR FORCE MICROCOMPUTERS

THESIS

Presented to the Faculty of the School of Systems and  
Logistics of the Air Force Institute of Technology  
Air University

In Partial Fulfillment of the  
Requirements for the Degree of  
Master of Science in Information Resource Management

Jay C. Sorensen, B.S.

First Lieutenant, USAF

December 1990

Approved for public release; distribution unlimited

## Preface

With the increasing usage of microcomputers and off-the-shelf software throughout the United States Air Force I felt that it was necessary to do an initial study of attitudes within the Air Force concerning software piracy. By completing this study, I felt that I could determine whether or not the Air Force's policies and regulations were indeed preventing software piracy.

Through an attitudinal survey and a review of Air Force literature, including numerous personal correspondences with Air Force inspector generals and computer and legal personnel, it was determined that the Air Force has made some strides in preventing software piracy from occurring on its resources. However, the study also indicated that software piracy is still occurring, and that additional efforts must be made if the Air Force wishes to curtail software piracy altogether.

Throughout the research, numerous individuals have contributed greatly and put up with a lot from me. Lieutenant Colonel D.J. McBride provided numerous hours of support not only as advisor and editor, but also as my academic advisor while at AFIT. My classmates put up with my off-the-wall humor and often inflated ego.

However, the persons putting up with the most were my wife Tamie and my three children, Erin, Marilyn, and Glenn. Erin often expressed the family's attitude in the waning

days by constantly asking, "Dad, are you done with your thesis yet?" Yes Erin, I'm finally done and you get your daddy back while your mother finally gets a husband and friend back as a companion instead of a shadow huddled over the keys of a computer in the corner of the bedroom.

J. Chris Sorensen

## Table of Contents

	Page
Preface . . . . .	ii
List of Figures . . . . .	viii
List of Tables . . . . .	ix
Abstract . . . . .	x
I. Introduction . . . . .	1
Background . . . . .	2
Types of Liability . . . . .	4
Avoiding Liability . . . . .	5
Problem Statement . . . . .	7
Investigative Questions . . . . .	7
Definition of Terms . . . . .	8
Scope . . . . .	11
Limitations . . . . .	12
Summary . . . . .	13
II. Literature Review . . . . .	15
Overview . . . . .	15
U.S. Copyright Law . . . . .	16
Historical Perspective . . . . .	16
Additional Insights on Copyright . . . . .	20
License Agreements . . . . .	20
Copyright Infringement Penalties . . . . .	22
Software Piracy . . . . .	23
Technical Methods to Prevent Piracy . . . . .	24
Summary of Copyright Law and Issues . . . . .	25
Government, Department of Defense, and Air Force Issues . . . . .	25
Air Force Literature and the Copyright Law . . . . .	28
III. Methodology . . . . .	33
Overview . . . . .	33
Comparative Analysis Methodology . . . . .	33

	Page
Survey Methodology . . . . .	35
Survey Population and Size . . . . .	36
Survey Instrument . . . . .	38
Validity and Reliability of Survey . . . . .	39
Statistical Procedures . . . . .	41
Summary . . . . .	42
IV. Results and Discussion . . . . .	43
Overview . . . . .	43
Summary of Results . . . . .	43
Results of Literature Review in Answering Investigative Question #1: What is the Status Of Current Air Force Anti-Piracy Policies and How Do They Compare to the Standards of ADAPSO and the Rest of the Software Industry's Suggested Minimum Standards . . . . .	46
Software Industry Guidelines . . . . .	47
1) The Monitoring of Software and Which Machines the Soft- ware is Assigned To . . . . .	48
2) Spot Checking Employees . . . . .	48
3) Making Software Piracy Grounds for Dismissal . . . . .	49
4) Developing an Employee Education Program . . . . .	50
5) Involving Management in the Problem . . . . .	51
6) Obtaining a Signed Acknowl- edgement From the Employee of His Awareness of the Law . . . . .	52
Overall Score . . . . .	52
Overview of Survey Demographics . . . . .	53
Survey Results: Investigative Question #2, How Well Do Air Force Personnel Understand the United States Copy- right Law, Software Licensing Agreements, and Air Force Anti- Piracy Regulations? . . . . .	59
Summary of Results to Investigative Question #2 . . . . .	66



	Page
Survey Results: Investigative Question #3, To What Extent Do Air Force Personnel Perceive Software Piracy as a Problem on USAF Microcomputers? . . . .	67
Summary of Results to Investigative Question #3 . . . . .	74
Survey Results: Investigative Question #4, What Are the Attitudes of Supervisors/Commanders Concerning Software Copyright Infringement? . . . . .	75
Summary of Results to Investigative Question #4 . . . . .	79
Survey Results: Investigative Question #5, Under What Circumstances Do USAF Personnel Feel That Software Copyright/ License Infringement is Justified and/ or Legal? . . . . .	79
Summary of Results to Investigative Question #5 . . . . .	83
Survey Results: Investigative Question #6, What Efforts Can/Are Commanders, Supervisors, and the Air Force as a Whole Use(ing) to Prevent Software Piracy from Occurring on USAF Resources? . . . . .	84
Summary of Results to Investigative Question #6 . . . . .	87
Survey Results: Investigative Question #7, Do USAF Personnel Believe That Current Regulations and Guidelines Concerning Software Piracy Adequately Prevent Piracy From Occurring on Air Force Microcomputers . . . . .	87
Summary of Results to Investigative Question #7 . . . . .	92
Survey Results: Summary of Written Comments . . . . .	92
Conclusion . . . . .	94

	Page
V. Conclusions and Recommendations . . . . .	96
Overview . . . . .	96
Summary of Findings and Recommendations . . . . .	96
Recommendations for Change . . . . .	99
Implications to the Air Force . . . . .	103
Recommendations for Further Research . . .	104
Conclusion . . . . .	104
Appendix A: Signed Statement of Acknowledgement . .	106
Appendix B: Organizations Contacted for Thesis Support . . . . .	107
Appendix C: Computer Software Piracy Survey . . . .	110
Appendix D: Survey Results in Percentages Along With p-Values for 2-Sample T-Test of Means OFFICER vs ENLISTED . . . . .	115
Appendix E: Pearson Correlation Coefficients p-Values Under Ho: $\rho = 0$ . . . . .	124
Appendix F: Mean Survey Responses Along With p-Values for 2-Sample t-Test for Means Commander/Supervisor vs Non-Commander/Supervisor . . . . .	132
Appendix G: Summary of Written Results . . . . .	137
Bibliography . . . . .	144
Vita . . . . .	148

## List of Figures

Figure	Page
1. Total Years Active Military Service - Enlisted . . . . .	55
2. Total Years Active Military Service - Officers . . . . .	55
3. Frequency of Computer Usage - Enlisted . . . . .	57
4. Frequency of Computer Usage - Officers . . . . .	57
5. Types of Microcomputer Usage - Enlisted . . . . .	58
6. Types of Microcomputer Usage - Officers . . . . .	58

### List of Tables

Table	Page
1. Copyright History . . . . .	17
2. Cronbach Alpha Coefficients . . . . .	40
3. Distribution of Enlisted AFSCs (n = 73) . . . . .	54
4. Distribution of Officer AFSCs (n = 75) . . . . .	54
5. Officer Responses to Survey Questions for Investigative Question #2 . . . . .	61
6. Enlisted Responses to Survey Questions for Investigative Question #2 . . . . .	61
7. Officer Responses to Survey Questions for Investigative Question #3 . . . . .	69
8. Enlisted Responses to Survey Questions for Investigative Question #3 . . . . .	69
9. Mean Scores of Commanders/Supervisors and Non- Commanders/Supervisors (* statistically sig- nificant differences) . . . . .	77
10. Officer Responses to Survey Questions for Investigative Question #5 . . . . .	81
11. Enlisted Responses to Survey Questions for Investigative Question #5 . . . . .	81
12. Officer Responses to Survey Questions for Investigative Question #6 . . . . .	85
13. Enlisted Responses to Survey Questions for Investigative Question #6 . . . . .	85
14. Officer Responses to Survey Questions for Investigative Question #7 . . . . .	89
15. Enlisted Responses to Survey Questions for Investigative Question #7 . . . . .	89

Abstract

This study looked at the United States Copyright Law and its applications to computer software. The study looked at USAF policies and regulations governing the protection of copyrighted software. The literature review, including personal correspondence with inspector generals and computer and legal personal, indicated that the Air Force has numerous policies concerning software copyright and the violation of those copyrights (software piracy). These policies and regulations were compared to standards set by the software industry and the results suggested that the appropriate policies are in place, but in some instances, enforcement was lacking. An attitudinal survey was conducted with 125 enlisted personnel and 125 officers, with a 58.4 and 60.0 percent usable return rate. Using a simple 5-point Likert scale and "Yes/No" questions, no overall significant differences of attitudes were demonstrated between the two populations. While many of the respondents felt that there was a problem with software piracy, few claimed to be personally involved. Understanding of copyright laws and what can and cannot be legally copied on microcomputers was lacking, especially in the junior ranks. Overall, it was determined that entry level education and enforcement of policies governing software piracy need to be increased.

UNITED STATES COPYRIGHT LAW AND SOFTWARE PIRACY  
ON UNITED STATES AIR FORCE MICROCOMPUTERS

I. Introduction

In January 1985, Future Computing Inc. announced the results of a survey of 45,000 small computer owners. Future Computing reported that 50 percent of business software in use at that time was illegally copied (pirated) software. Future Computing estimated the value of pirated software in the neighborhood of \$1.3 billion through 1984 with \$600 million occurring in 1984 alone. In another survey, Infocorp reported that 22 percent of its respondents were using some pirated software and that 6 percent of the computer owners used pirated software as their main software source at an estimated value of \$160 million in 1984 (3:35; 5:18; 26:23; 30:179; 34:8; 36:1). It is reported today that the problem has further escalated and that the total impact of software piracy to the computer industry now amounts to \$4.1 billion annually (33:111).

Research has indicated that software piracy is one of the major problems facing the \$50 billion a year software industry (37:23). "People who wouldn't think of shoplifting a software product on their lunch hour don't think twice about going back to the office and making several illegal copies of the same software" (9:43). Similarly, "...most

employees would not take a \$200 typewriter home with them from the office which is, in essence, equivalent to making copies of software for which they have not paid" (3:35). Spurring the problem of software piracy is the fact that end-user computing is becoming a popular phenomenon. Users are coming more in contact with software that is not only beneficial on the job, but can also be used on home personal computers. There appears to be an association between software piracy and the increasing number of end-user computing systems (27:19; 50:5). As a user of software and a proponent of end-user computing, the Air Force and its employees are facing the software piracy issue just as American business is. Therefore, it is essential that Air Force personnel understand the laws that are relevant to computer software and how those laws pertain to them. It is also essential that the Air Force has a strong anti-piracy policy to prevent software piracy from occurring on its microcomputers.

#### Background

Recent lawsuits have suggested that the software industry is no longer going to accept software piracy as an uncontrollable problem (42:1; 43).

The general notion of software piracy as an unethical practice is being driven home by expensive lawsuits brought against major corporations and other offenders pirating software. (33:107)

In 1984, Lotus Development Corporation sued Rixon Company for copying its Lotus 1-2-3 software package. While the

suit was initiated for a sum of \$10 million, the case was settled out of court for an undisclosed sum and the return of all illegal copies of the software (3:31; 5:16; 7:42,46; 8:43; 11:74; 26:28; 30:184; 31:58). In 1985, Lotus was again in court pursuing a software copyright lawsuit. This time Lotus was suing Health Group Inc. of Nashville, TN. In this lawsuit, Lotus named, in addition to the corporation, many of the corporation's board members as well as company management information systems directors. Following that suit, Lotus sued Mueller Company Inc., naming Mueller's data processing corporate manager along with several others in the suit.

Like Lotus, MicroPro International has taken software pirates to court. MicroPro, with the assistance of the Association of Data Processing Service Organization, Inc. (ADAPSO), in a 1985 lawsuit, sued Wilson Jones Co. for copying portions of its popular Wordstar program. The lawsuit, like others, named specific names. MicroPro was seeking \$500,000 in damages. Again, the case was settled out of court for an undisclosed amount of money (5:16; 7:46; 36:8). Additionally, the Software Publishers Association (SPA) reported in February 1990 that it had brought 30 lawsuits against software pirates in just the last 20 months. In June 1989, SPA won a six-figure out-of-court settlement for five software vendors against a publishing firm on the grounds that the company had been using pirated software (33:107, 111). Also in 1989, Novell Inc. reached an



out-of-court settlement for a 'substantial sum' from Vicom Inc., on the grounds that Vicom had pirated Novell's software and distributed those copies to several of Vicom's customers (35).

It is clear from the above cases that software vendors are determined to put an end to software piracy. The companies have taken a firm stand and are hoping that their tactics will pay off in the reduction of software piracy, and it appears that in some ways they are. To illustrate, in a 1989 survey of the 1988 Fortune 500 Companies, one corporate employee stated that it is cheaper to have a liberal software purchasing policy than it is to pay legal fees and potential fines. This is easily understood when one considers that a single fine of \$50,000 would purchase some 150 copies of Lotus 1-2-3 (3:35).

Types of Liability. Three basic types of liability exist under the Copyright Law, corporate liability, contributory liability, and criminal liability. Corporate liability is incurred if a direct financial benefit is gained for the business by the employee illegally copying software. Contributory liability suggests that a supervisor had something to do with the employee copying the software package. This could be something as simple as an off-the-cuff suggestion that a program be copied. Criminal liability occurs when there is willful violation of the Copyright Act for financial or commercial gain (11:75-76).

Avoiding Liability. To free itself from these liabilities, an organization (including federal agencies because the Government has waived sovereign immunity with regard to copyright and patent issues (29)) must develop a strong program to prevent software piracy from occurring in the work place.

In light of recent court actions, it is imperative that

...internal auditors ... take steps to determine and document the extent of unauthorized copying of software within their organizations. Such actions may reduce the possibility of litigation arising from the misuse of software within an organization. (8:47)

In addition, general managers, and specifically information systems managers, must establish strict piracy policies that will be strongly enforced if businesses wish to keep their employees from violating the Copyright Act while relieving themselves of potential liabilities (42:3).

However, policies alone will not prevent an organization's employees from pirating software. The organization must pay constant attention to its software resources. It is apparent that these policies, "when policed and enforced, arguably remove(s) the copying activities from the scope of employment and renders the activities personal in nature for which the employer is not liable" (11:75). ADAPSO has sent a letter to major corporate executives urging the development of firm anti-piracy policies. ADAPSO has threatened more litigation if such policies are not developed (3:31; 11:74-77; 26:25; 36:8).

According to current surveys, it appears that American businesses are taking these threats seriously. Clevenger reports that 72 percent of his respondents have current policies regarding copyright violation (8:42-47). Athey reports from her survey that 88 percent of her respondents have policies regarding copyright violation. These policies vary as to whether the duplication is for work, home, or personal use. Athey's survey also indicated that the primary penalty for violators of these company policies was verbal or written reprimands with only three percent terminating employment after the second incident (3:31-35).

ADAPSO, SPA, software companies, and other businesses have provided suggestions to prevent software piracy in the work center. A suggested base for a piracy prevention program should involve: 1) the monitoring of software and which machines the software is assigned to, 2) spot checking employees, 3) making software piracy grounds for dismissal, 4) developing an employee education program, 5) involving management in the problem, and 6) obtaining a signed acknowledgement yearly from the employee of his awareness of the law (8:44; 26:23; 33:111; 36:8; 42:24; 43). ADAPSO has provided a form letter to over 75,000 firms suggesting that the policy statement in Appendix A be signed by all the members of an organization to help curb software piracy. By implementing and enforcing these policies, ADAPSO and SPA indicated that an organization would be adequately

protecting itself from litigation should an employee be caught participating in software piracy.

### Problem Statement

Although Air Force policies and regulations concerning software piracy exist, it is not known if these policies/regulations are sufficient or if they are understood and applied appropriately in the field. This thesis will attempt to determine if the Air Force's anti-piracy program adequately meets the guidelines prescribed by the Association of Data Processing Service Organization Inc. and the software industry, and if the anti-piracy program successfully prevents software piracy on USAF microcomputers.

### Investigative Questions

The research for this thesis will address seven specific questions to resolve the aforementioned problem statement. The investigative questions are:

- 1) What is the status of current Air Force anti-piracy policies and how do they compare to the standards of ADAPSO and the rest of the software industry's suggested minimum standards?
- 2) How well do Air Force personnel understand the United States Copyright Law, software licensing agreements, and Air Force anti-piracy regulations?
- 3) To what extent do Air Force personnel perceive software piracy as a problem on USAF microcomputers?

4) What are the attitudes of supervisors/commanders concerning software copyright infringement?

5) Under what circumstances do USAF personnel feel that software copyright/license infringement is justified and/or legal?

6) What efforts can/are commanders, supervisors, and the Air Force as a whole use(ing) to prevent software piracy from occurring on USAF resources?

7) Do USAF personnel believe that current regulations and guidelines concerning software piracy adequately prevent piracy from occurring on Air Force microcomputers?

#### Definition of Terms

A brief listing of unique terms used throughout this thesis are here defined. The definitions provided are common definitions within the software industry.

The term **software** is often used interchangeably with the term program, i.e., to refer to a 'set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.' (37:21)

**Software** includes,

1. The basic algorithms or methods implemented in the program
2. The program itself in source code and object code versions
3. The supporting documentation, including program descriptions, flow charts, instruction manuals, operator's manuals, and other materials that explain the operations of the program (37:22)

**Source code** is the way that the programming code appears after having been written by the programmer.

Object code is the way the code looks after being assembled or compiled into the computer.

"Operating Systems Software consists of the programs necessary to manage and control the basic internal function of the computer..." (10:15)

Application software consists of those programs designed for the specific application or end use of the computer, such as word processing, order entry, or highly specialized applications for specific industries... Application software also includes certain types of communications software. (10:15)

Mass marketed, micro-based software is aimed at the everyday or common user, "is usually designed for microcomputers, and is marketed to end-users primarily through retailers or by mail order" (10:15).

Software piracy is the reproduction of copyrighted/ licensed software for purposes other than those granted under the copyright law or license agreement. Generally, this includes all copies other than those for archival purposes or to place the program into machine readable code. (ADAPSO likes to distinguish between software piracy, which they claim is "when organizations choose consciously to encourage, or unconsciously to allow employees to make and use illegal software copies" (43) and softlifting which they refer to when discussing individuals involved in private software piracy for personal gain or to help out a friend. (10:16))

To explain the methodology for software protection, Scott, a noted computer law expert, indicates that copyrights protect programs while patents do not.

**Copyright and patent protection** are not mutually exclusive; neither are copyright and trade secret protection. Copyright protects the expression of an idea; patent protects the embodiment of an idea; trade secret can protect the expression, embodiment, or idea itself. Neither copyright nor patent law provides protection for ideas per se. (37:26,210)

Cooper, a noted software lawyer, further distinguishes between the different methodologies of software protection.

**Patents** confer a limited monopoly upon the patent owner who has the exclusive rights to make, use, license, and sell the embodiment of an invention for 17 years. Patent laws protect the idea of the invention as well as the invention itself even against innocent persons whose infringement arises out of independent creation. (10:7)

**Copyright** protects the form of expression of any work of authorship that is fixed in a tangible medium. Copyright protects only against actual copying of the form of expression, and not against the use of ideas embodied in the expression or against independent creation of the same or a similar work. (10:7)

**Trade secrets** are secret information and ideas used in a trade or business that give the owner a competitive advantage. Trade secret protection is not lost by disclosure of the trade secret, provided that the disclosure is only under circumstances where there is a legal duty of the recipient to safeguard the confidentiality of the trade secret. The protective interest continues for so long as the secret is maintained, but is forever lost when the secret becomes general knowledge. (10:7)

While attempts to apply patent and trade secret protection to software have been made, it is generally accepted that they do not apply to the mass-marketed micro-based

software that is within the scope of this thesis. For example, trade secrets become null and void once the secret is disclosed to the public. Since this thesis addresses mass marketed software, it should be clear why trade secret protection would not be the best way to protect one's software (26:29). Because of the lengthy process of getting a patent, its relatively short term (17 years compared to a copyright's 50 years), and the necessity to prove that it has never before been invented or patented, few developers have sought to protect application software with a patent. Ultimately, it was Congress that decided that copyright should be the method of software protection when it included the term software in the latest amendments to the Copyright Law of 1976 (25:54). Therefore, let it suffice for now that copyright is the primary accepted method for protecting software from illegal duplication.

### Scope

The scope of this thesis is limited to microcomputers using mass-marketed, micro-based software under use by the Air Force in the continental United States. This limitation is based upon the fact that outside of the continental United States, software copyright laws diverge greatly and are much more complex to understand. The limitation to mass-marketed software is due to their popularity within the Air Force for end-user computing, as well as their commonality on home/personal systems. Other types of software,



for example contracted software, have governing federal regulations and policies far beyond the scope of this thesis. Software for mainframe computers is also not addressed due to the difficulty in copying said software as well as the relatively small amount of software used for end-user computing as compared to that used on microcomputers.

Air Force units have purchased thousands of copies of various software packages, both application and operating system, for use on its microcomputers at a cost reaching into the millions of dollars. As a result, this represents the area of greatest vulnerability for the Air Force in that individuals/organizations are much more likely to copy popular micro-based software than anything on mainframes or that was developed for narrow purposes. This research, despite the limitations of its scope, will provide insight into the Air Force's policies against, and its ability to prevent, software piracy on its computer systems.

### Limitations

While the research procedure as a whole should provide enlightening information, it should be noted that there will be one major limitation to the research process. This limitation, as with many procedures using surveys, will be based upon the honesty of the respondents. The research could result in incriminating information for the Air Force and its members. Therefore, it is possible that a complete understanding of the effectiveness of the Air Force's

policies and regulations may not be totally possible if respondents feel that they face potential retribution. It is hoped that a guarantee of anonymity will keep the effect of this limitation to a minimum. Additionally, any research that is based on perception always runs the risk that perception doesn't match reality. Unfortunately, we have no practical way to get at reality. However, since the survey methodology of this paper is an acceptable research procedure that has been used in the past, it is hoped that the findings at least somewhat mirror reality (2; 3; 38; 39; 41).

#### Summary

It is clear from the literature that the United States Air Force should develop and enforce an anti-piracy program. This will not only help prevent potential lawsuits, but also enable the Air Force to maintain a working relationship with the software industry.

This thesis will assess the existing Air Force policies concerning software copyright violations as well as determine the perceived effectiveness of the Air Force's anti-piracy efforts. Through answering the seven investigative questions, the status of the Air Force's program to prevent software piracy on its microcomputers should be clear.

The remaining portions of this thesis are divided into four chapters. Chapter II is a literature review of existing journals, research papers, popular magazines, as well as

a thorough review of Air Force regulations and policies. This literature review answers investigative question #1 while providing additional insights and background on the software piracy issue.

Following the literature review, chapter three outlines the methodology used to answer the investigative questions. It explains the survey technique as well as the statistical methods used to answer investigative questions #2 - #7.

Chapter four presents the results from the survey as well as summarizes the findings from the review of Air Force literature. After presenting the overall results, the chapter goes on to answer each of the investigative questions.

The fifth and final chapter sums-up the final conclusions in an abbreviated format. Additionally, the chapter presents recommendations to the Air Force for improving its position with regard to software piracy and suggests some additional follow-on research.

## II. Literature Review

### Overview

Computers were introduced in the mid-1900s, and have since developed at a phenomenal rate. The development was so fast that governing laws could not keep pace. Computer law was basically ignored in the 1960s and 70s. For a time, legislation was being considered that would slow down computer development in order to allow Congress to catch up to the situation at hand. However, Congress decided that this would not be in the best interest of business or the United States. In the 1980s, amendments to the Copyright Law were passed by Congress (37:13-14).

Research for this chapter clearly suggests that the software industry is protected by copyright law in addition to numerous other laws that are beyond the scope of this thesis. This review of the literature provides a background of the copyright law and an understanding of software licensing agreements. The chapter also outlines the various liabilities for copyright violation. The chapter also explains software piracy and what different groups such as ADAPSO are doing to curtail the problem. The chapter concludes with an extensive review of Government, Department of Defense (DoD), and Air Force regulations with regard to software copyright and license infringement.

## U.S. Copyright Law

When Congress passed the 1980 Amendments to the Copyright Act of 1976, computer programs were considered protected at the moment of creation under federal copyright law. Owners of software copyrights have the right to copy their works, prepare derivations of the original work, distribute their works through sale, rental, leasing, and lending, and perform and display their works in public. If a person (or company) does any of the aforementioned without the copyright owner's permission, then a copyright infringement has occurred (26:28; 42:10; 48:8).

Historical Perspective. In 1790, Congress passed the first copyright legislation in the United States. This Act was limited in scope and has been amended and rewritten several times. Table 1 provides a synopsis of these changes.

As Congress was trying to develop a modern version of the Copyright Law, numerous changes began to take place in technology. The United States had entered into the technology revolution. In 1964, the Copyright Office received for the first time a computer program for registration. These programs were simply the written code of the program as existing law required that a copyrighted work be readable by the human eye (37:36,39).

As computers were being developed, no one really foresaw a concern for copyrighting software programs. Most computers being developed through the 1960s were being

Table 1. Copyright History

Year	Changes to Law
1790	First U.S. Copyright Law; protected maps, charts, and books
1802	Rights extended to designs, engravings, and etchings
1819	Supreme Court and Circuit Courts given jurisdiction
1831	Repealed 1790 Act, extended rights to musical works
1834	Copyrights to be recorded as deeds
1856	Dramatic works added to the list of protectable items
1859	Dept of Interior given responsibility of copyright
1865	Copyrights grantable to photographs and negatives
1870	Library of Congress given responsibility; rights extended to paintings, drawings, chromo, statues, statuary, and models or designs intended to be perfected as works of fine art
1909	Repealed all prior laws; extended length to 28 years for both initial and renewal terms; established Office of Registry of Copyrights under the Library of Congress
1947	Established Title 17 of the United States Code
1976	Codified existing law; extended length to 50-75 years
1980	Software Amendments added to cover computer programs

(Source, Title 17, USC (45))

developed as bundled packages. That is to say, both hardware and software were sold as one package. Software that worked on one computer did not usually work on another. Software companies complained, and anti-trust lawsuits were filed. Since IBM was the leader of the industry, the finger was pointed at them. In 1969, IBM announced its intent to unbundle its computer packages, leading to exponential growth in the software industry. In addition, the advent of microcomputers, video games, and the declining price of hardware further spurred the industry's growth (37:24).

In 1976, the first major revision of the 1947 Copyright Law was enacted. The law has become known as the United States Copyright Act of 1976 and was established under PL 94-553, October 19, 1976, 90 Stat 2541. This law codified and reenacted the 1909 law as positive law and provided an effective date of 1 Jan 1978. The law also extended the length of a copyright to the life of the author plus 50 years for initial copyrights and 75 years for renewals (45:v,vi,viii).

The 1976 Act did not protect "computer programs" per se, but instead left the existing level of protection, as already interpreted by the courts, as status quo. It was apparent that both legislative history and congressional intent expected computer software to be included under the Act (37:36,39). Instead of addressing the issue at a time of uncertainty and phenomenal change in the computer industry, Congress established the National Commission on New Technological Uses of Copyrighted Works (CONTU). Congress instructed CONTU to develop guidelines for revisions of the Copyright Act to include computer software. Congress gave the commission three years (later changed to three years and seven months) to develop its recommendations (48).

CONTU developed three major recommendations for revision of the 1976 law. The recommendations were

...to make it explicit that computer programs, to the extent that they embody an author's original creation, are proper subject matter of copyright;  
...and to ensure that rightful possessors of

copies of computer programs may use or adapt these copies for their use. (48:1)

CONTU's recommendations were codified in the 1980 Software Amendments under PL 96-517, 12 Dec 1980. The amendments replaced Section 117, thereby removing the status quo of software and providing specific rights to copyright owners. The definition of "computer program" was added, and limited copying rights for archival purposes or essential to utilization of the program with the computer were established (4:6-7; 37:310; 42:10).

An alarming, precedent-setting court case for the software industry came in 1988 when a lawsuit involving BV Engineering and the University of California at Los Angeles resulted in state agencies being found exempt from copyright law. Software companies immediately realized that this case could open up numerous legal loop-holes that would make it easier for users to legally use copyrighted software without providing the copyright owner due compensation. As a result, several software lobby groups are hoping for another amendment to the copyright law that will include the issue of state agency exemption. However, due to sovereignty issues at hand, and the fact that the Supreme Court refused to hear the case in 1989, it appears highly unlikely that the software industry will be able to get Congress to set such an overwhelming precedence over what many would deem a minor issue (33:111).



Additional Insights on Copyright. In addition to the software amendments, additional copyright issues are addressed in the copyright law. In particular, the fair use doctrine and first sale doctrine both have significant impact on computer programs.

The doctrine of fair use is specifically included in Section 117 of the 1976 Copyright Act: 'Notwithstanding the provisions of section 106, the fair use of a copyrighted work, including such use by reproduction in copies ... or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. (37:347)

In addition to the fair use doctrine, the first sale doctrine is also outlined in the Copyright Act. First sale doctrine gives a copyright owner the right to distribute his work. Once sold, the copyright owner no longer has a say as to what the purchaser does with the work short of reproducing the work. The purchaser may sell or rent the work and the copyright owner has no say in the matter. However, license agreements may preclude the rights established within the first sale doctrine (8:44; 37:341-342).

License Agreements. While license agreements are not addressed by the Copyright Law, the agreements are an extension of authority resulting from that law. License agreements are covered by state governed legislation and further protect a copyright owner's rights while restricting those of the licensee.

Most software, when originally purchased, comes packaged in a sealed envelope. The buyer is often forewarned that breaking the seal signifies acceptance on the part of the buyer to agree to the terms of the license. This license often indicates that the buyer is not the sole owner of the software that he is purchasing. Ownership often remains with the software vendor and the buyer in turn is not really a buyer, but only a licensee. A license usually maintains right of ownership, or title, of a software package with that of the author or software company. The license grants permission for use, and archival and machine readable code backup. No permission is granted for modification of the program. Most agreements also strictly forbid the use of a software package on a local area network system (LANS). Often, the rights of the first sale doctrine are removed in that the licensee may not be able to sell or transfer the package. Upon termination of the agreement, the license will often require that the software package be returned to the company or destroyed.

The authority of these agreements varies from state to state (8:45; 11:74). While there have been many court cases challenging the validity of these so called "shrink wrap license agreements," the courts are apparently upholding the rights of the states to enact such legislation as evidenced by Louisiana's Software License Enforcement Act (4:9; 7:46).

Copyright Infringement Penalties. In addition to the background and content of the law, it is imperative that software users understand the penalty for violating the law. All violations of the United States Copyright Act fall within the jurisdiction of the federal court system. Once charges have been filed under the Copyright Law, either statutory or criminal, the court can impound all copies and originals of software packages involved until after the trial. If the defendant is found guilty of copyright infringement, then the court can order the destruction of all copies and originals (37:382-385).

The plaintiff has the right to recover actual damages, including lost profits, or statutory damages. At present, statutory damages for simple infringement are set at \$250 to \$10,000 for each work involved. If willful infringement is proved, suggesting that corporate benefits or personal financial gain was achieved as a result of the infringement, then the fines can be extended up to \$50,000 per copyrighted work. In addition, the defendant can be ordered to pay all attorney fees and court costs involved with the trial (37:382-385; 8:45; 33:107; 43).

Criminal penalties are similar to that of statutory penalties. For willful infringement for financial gain, a defendant can receive a fine of up to \$10,000 and one year imprisonment. In addition, all involved software can be impounded along with all the equipment used to make the copies or used to run the illegal copies (37:387).

In retrospect, one should note that current copyright law is not written to sufficiently cover forthcoming technological changes. "In the near future, increasing reliance on information storage and retrieval devices, communications, satellites, and laser technology no doubt will make even greater demand on copyright" (45:v).

Having explained the United States Copyright Law and its implications to computer programs this review will now address the issue of software piracy.

### Software Piracy

Software piracy appears to have reached epidemic proportions in home computers, and on small and large business systems. Having grown out of hand in the civilian sector, it is possible that the software piracy problem could also exist in the United States Air Force and throughout the Department of Defense. As mentioned at the first of this paper, pirated copies of software may include as much as 50 percent of the software in microcomputers today, and some reports even suggest that the number could be "as high as five illegal copies for every legal one" (33:111). This paper will now address the questions, "just what is software piracy, who's to blame, and how can it be prevented?" (3:35; 5:18; 34:28).

Pirated software is simply software that has been copied for use other than archival purposes or to place the program into machine readable code without the copyright

owner's permission, and is used outside of the fair use policies of Title 17, USC (45).

Technical Methods to Prevent Piracy. In the past, software vendors have attempted to prevent piracy through various means, most of which have met with disfavor by software users. Just to illustrate, "One organization estimates that it spends \$50,000 in time and money recovering/replacing copy protected software... " (3:35). As a result of these high costs, some companies have now developed policies that prohibit the purchase of copy protected software (i.e., software that can only be copied onto one machine, one time and is altered such that it cannot be copied again). Once copy protected software is damaged or lost, a replacement package must be purchased since the original was altered at installation and cannot be reinstalled without the ability to re-alter the program (3:31-35; 5:20; 11:73).

Most software companies no longer copy protect their software via technical means because of the ease of circumvention and because the public stops buying their product. Instead, software vendors are hoping that the copyright law, accompanied with strong court cases, will relieve the losses from software piracy. If the legal avenue fails, the software industry may be forced to introduce new and more effective (along with more burdensome) methods of copy protection (5:20; 31:59).

While technical methods of software piracy remain possible, the software industry hopes consumers will begin to abide by the precepts of the copyright law and eliminate the need for burdensome copy protection mechanisms all together.

#### Summary of Copyright Law and Issues

This literature review has taken a look at the United States Copyright Act and its implications for computer software. The software industry hopes that computer users will now place themselves in compliance with the law. In fact, ADAPSO has tried to clear up some of the myths often circulated to justify software piracy in hopes of helping users to understand the significance of the law. ADAPSO points out that

...software developers do not condone unauthorized copying in order to gain market penetration...the price of software does not make unauthorized copying justifiable...and rationalization for software piracy does not make it right or legal. Some people say, 'the product is too expensive.' The price set by the developer and retailer does not give someone a license for theft. (43)

#### Government, Department of Defense, and Air Force Issues

The United States Government and its employees are affected somewhat differently than civilians and American business with regard to the United States Copyright Law. The Government has sovereign immunity from prosecution for violating federal statutes unless the Government chooses to waive said immunity. With regard to copyright and patent

issues, the U.S. Government has chosen to waive immunity, and as such, can be sued for violating the copyright law within certain guidelines and stipulations (29). Under Title 28 U.S.C. 1498b, the Government can be taken to the federal Court of Claims by a plaintiff charging the government with copyright infringement. The Court of Claims judges statutory cases and can fine the Government for "entire compensation as damages for such infringement, including the minimum statutory damages..." (47). Also, no injunctive relief, i.e., cease and desist order or destruction of software, may be sought from the Government as a result of Title 28 (29). Under Title 28, Government employees working for and in behalf of the Government who commit a copyright infringement within the duties of their jobs are granted immunity from both civil and criminal prosecution (15:11). The one major exception to this would be if an individual copies Government purchased/leased software for personal use or gain. Under these circumstances, an individual would be found operating outside of the scope of his job and thus the protection of the Government. It should also be noted that while an individual might be exempt from prosecution under Title 17 U.S.C., that individual could still receive administrative punishment from his governing agency, which could result in a stiffer penalty than if charged under Title 17 U.S.C. (For military personnel this would be under Article 92 of the Uniform Code of Military Justice (UCMJ). (44)) Under UCMJ Article 92, an individual

could receive a dishonorable discharge, be incarcerated, and receive a substantial penalty for violating regulations that forbid copyright infringement (44).

Software purchased/leased by the Air Force for its microcomputers is often acquired under the guidelines of the Federal Acquisition Regulation (FAR) and the Department of Defense Supplement to the FAR, known as the DFAR (23; 24). Part 27 of the FAR and Part 227 of the DFAR specifically address acquisition of software. These parts also provide some unique definitions used within both regulations (12). The FAR acknowledges the fact that "The Government honors rights in patents, data, and copyrights, and complies with the stipulations of law in using or acquiring such rights" (24:Part 27.104(g)).

To clarify its position toward software rights in acquisition, the FAR includes commercial and copyrighted software under the category of "restricted computer software." As such, the Government claims "restricted rights" to commercial or copyrighted software which essentially entails the same rights as those provided under the current Copyright Law, i.e., the right to make archival back-ups, to place the software into machine readable code, and other rights granted. Additionally, the Government claims a right to place software onto additional machines should the original be out of commission, provided that no more than one copy is being used at a given time. The Government also claims a right to modify software as long as the original



work is protected (24:Part 27.401, 27.404(e), 52.227-19; 23:Part 227.471; 46).

The government has sought to protect copyrighted software because

...protection of such data from unauthorized use and disclosure is necessary in order to prevent the compromise of such property right or economic interest, avoid jeopardizing the contractor's commercial position, and preclude impairment of the Government's ability to obtain access to or use of such data. The protection of such data by the Government is also necessary to encourage qualified contractors to participate in Government programs and apply innovative concepts to such programs. (24:Part 27.402(b))

It should be clear from the review of Government literature up to this point that the United States Government supports the rights of copyright owners. This support is beneficial to both parties. This paper now turns to Air Force specific literature to see how far the Air Force is going in its support of copyright issues.

Air Force Literature and the Copyright Law. There are at least four Air Force regulations (AFR) that address the issue of copyright and its implications to the Air Force and its employees. AFR 110-8, Inventions, Patents, Copyrights, and Trademarks, is the Air Force's governing regulation that addresses copyright questions. In general, the regulation points out that "It is Air Force policy to recognize that a copyright owner has a legally enforceable property right" (15:7). This regulation also refers the reader to Title 28 and specifically states that "...Air Force personnel who may

infringe upon the rights of a copyright owner in connection with their Government employment are not personally liable for such infringement" (15:11). Other than these two points, the regulation says nothing else with regard to copyright law and does not specifically address the software issue. However, there are other Air Force regulations that cover copyright issues and which specifically address the software question.

The primary regulation which addresses copyright issues and computer software is AFR 205-16, Computer Security Policy (13). The following is a brief synopsis of the regulation and its specific points of interest:

Do not reproduce vendor supplied software, except as permitted by the terms and conditions of the contract. Do not violate copyright laws. (13:7)

Concerning the use of personal computer software on Air Force equipment, the regulation stipulates that "...the commander must consider copyright laws...(13:8)" Concerning Joint Service Activities, a memorandum of agreement must ensure that "There is no violation of software copyright laws" (13:8).

Because the Air Force has a policy against fraud, waste, and abuse, the regulation defines fraud and abuse in relation to software issues, suggesting that software piracy could fall into either one of these two definitions.

Fraud. Any intentional deception designed to unlawfully deprive the Air Force of something of value or to secure from the Air Force for an individual a benefit, privilege, allowance, or consideration the which he or she is not entitled.

Abuse. Intentional, wrongful, or improper use of Air Force resources. (13:30)

Additionally, the regulation goes on to state

Copyright restriction. Do not violate copyright laws. Make sure personnel are aware of copyright restrictions placed on automated system software. Ensure users know and understand these restrictions. (13:30)

and

Make sure the use of government-owned or government-leased software is consistent with copyright agreements. Prohibit the use of pirated software. (13:61)

This regulation also discusses the importance of conducting a risk analysis on small computers which is to include software protection from fraud, waste, and abuse. The regulation states that training and awareness is critical for all computer users. It further stipulates that training is to include prohibition of fraud, waste, and abuse as well as the penalties for the violation of this regulation. Initial training is to be conducted at Basic Military Training School and through all of the various officer accession programs (13).

Violation of this regulation is punishable under UCMJ Article 92 (13:1), and as such an individual could receive a dishonorable discharge, forfeiture of all pay and allowances and confinement for up to two years (44:IV-28). These potential penalties should be a strong deterrent to software piracy--if Air Force personnel are truly aware of them and if they are used when an individual is caught involved in software piracy.

Two other Air Force regulations make specific references to software and the copyright law. AFR 700-26, Management of Small Computers, states that "Copying commercially purchased software, without a license agreement, for other than back-up purposes, is illegal" (16:6). AFR 700-10, Information Systems Security, clearly states one reason why the Air Force is to adhere to copyright laws. "Misuse of information systems resources violates the public trust placed on both military and civilian government employees...and can publicly embarrass the Air Force" (14:3).

Several of the major commands of the Air Force have added their own supplements to AFR 700-26. Highlights from some of these supplements are here included to emphasize the effort that the major commands are making to stop software piracy from occurring in their work centers.

Strategic Air Command's (SAC) supplement gives specific instructions as to how software piracy is to be prevented from limiting the number of copies to be made to identifying who maintains and catalogs the originals. This supplement further states that copyrights are to be honored and that all users are to be briefed on penalties for misuse of Government computer resources. The supplement also contains an extensive inspection checklist to ensure that SAC's policies are being implemented (21).

Military Airlift Command's (MAC) supplement addresses such issues as making back-up copies and securing them from unlawful use. The MAC supplement stipulates that upon

upgrading a software package, the obsolete versions will be destroyed to prevent unlawful usage. Fraud, waste, and abuse are addressed with the specific mention of not violating licensing agreements. Probably the most important directive from the regulation is that the organization's small computer manager is to "Make random periodic checks to ensure compliance with Air Force and MAC directives" (19:6).

Air Force Communications Command's supplement to AFR 700-26 basically restates the guidelines of AFR 700-26 as well as the guidelines from the FAR and DEAR (17).

Pacific Air Force Command, Space Command, and Air Force Logistics Command have also supplemented AFR 700-26. Essentially, these supplements simply clarify one more time that users are not to violate the copyright law and that commanders/supervisors have a responsibility to ensure that software piracy does not occur in the work center (18; 20; 22).

As can be seen from the review of the government literature, it is clear that the Government, the Department of Defense, the Department of the Air Force, and the lower commands have all made an effort to establish firm policies with regard to software piracy. Now the question arises, are these policies, regulations, and guidelines accomplishing the desired objective? The means used to determine the answer to that and the other investigative questions is addressed in the next chapter.

### III. Methodology

#### Overview

This thesis attempts to determine if the Air Force's anti-piracy program adequately meets the guidelines prescribed by the Association of Data Processing Service Organization Inc. (ADAPSO) and the software industry. This research was used to determine if the Air Force's efforts to prevent software copyright infringement on its computers are successful.

Generally speaking, the research methodology took a two-pronged approach. First, a comparative analysis was conducted contrasting software piracy prevention programs/guidelines within the civilian sector to the Air Force's existing copyright infringement regulations and policies. The second portion of the research entailed a survey of Air Force personnel. The survey determined USAF members' perceptions of Air Force regulations and policies concerning software piracy. Inferences were made from the survey concerning the effectiveness and adequacy of the Air Force's efforts to prevent piracy from occurring on its microcomputers.

#### Comparative Analysis Methodology

The comparative analysis portion of the methodology addressed the Air Force's policies and regulations concerning software copyright infringement. These policies and

regulations were analyzed in the context of current United States copyright law and software piracy prevention guidelines within the civilian sector. This qualitative and subjective analysis provided a basis for the survey portion of the research. The comparative analysis also answered the first investigative question, that of whether or not the Air Force's efforts to prevent software piracy meet the minimum requirements of ADAPSO and the software industry.

Along with a thorough library search, numerous civilian organizations were contacted for assistance in providing literature and information to assist in the comparative analysis. These organizations and individuals included professional societies, lawyers, college professors, and editors of prestigious journals involved with pertinent issues. The individuals and organizations are listed in Appendix B.

The final part of the comparative analysis involved an examination of the Air Force's regulations and policies concerning software piracy. These regulations and policies were scrutinized to determine if they provide sufficient policy to meet ADAPSO's and the software industry's minimum suggested requirements for a piracy prevention program: 1) the monitoring of software and which machines the software is assigned to, 2) spot checking employees, 3) making software piracy grounds for dismissal, 4) developing an employee education program, 5) involving management in the problem, and

6) obtaining a signed acknowledgement from the employee of his awareness of the law (8:44).

In addition to the standard Air Force publications, several Air Force organizations were contacted for regulations, policies, and directives that might have been issued from their respective organizations concerning software piracy. All major command (MAJCOM) inspector generals (IG) were contacted for releasable inspection reports as well as guidelines issued from their offices. All MAJCOM small computer technical centers (SC) were also contacted for any guidelines/directives that they might have issued. The Air Force Office of Special Investigations as well as the Judge Advocate General were contacted to determine if there had ever been a member of the Air Force charged and/or punished for violation of the Copyright Law or Air Force regulations governing software piracy. Additionally, the Air Force Communications Computer Security Management Office (AFCSMO), which is responsible for programs to prevent software piracy on Air Force resources, was also contacted for input into the comparative analysis.

#### Survey Methodology

While the comparative analysis methodology determined the adequacy of the Air Force's anti-piracy efforts (investigative question #1), the survey portion of the methodology assessed the effectiveness of the Air Force's program in preventing software piracy from occurring on its



microcomputers. The survey methodology answered investigative questions #2 - #7. The survey addressed a cross-sectional viewpoint of the respondents at the time they answered the questionnaire. The goal was to obtain a current understanding of the situation and not what it had been in the past. The reason for looking at the situation today was based upon the assumption that users are more aware of the copyright laws today than in the past. The use of a survey methodology is supported historically by five similar surveys used by civilian researchers who were desiring similar information from civilian organizations (2; 3; 38; 39; 41).

Survey Population and Size. With the increased use of microcomputers throughout the Air Force, it is not unlikely that the majority of personnel in the Air Force today will at some time in their career use a microcomputer. Therefore, it was important to gain an understanding of software piracy perceptions and attitudes toward pertinent policies from a representative sampling of all Air Force personnel.

There were two populations surveyed for this part of the research. The survey populations included all Air Force enlisted personnel in the first population, and all Air Force officers for the second population, all within the continental United States. Due to the existing policies established at the USAF Military Personnel Center (MPC) the survey size for each population was set at 64. This number is obtained by using a general formula to achieve a

reliability level of 90% +/- 10%, which is the highest level of reliability currently allowed by MPC. At this rate, one can feel 90% confident, +/- 10%, that the responses of those surveyed truly reflect the entire population's attitudes. Using the allowed sample size of 64 and estimating an approximate 50 percent return rate, the number of surveys sent out to each population was 125. By breaking the survey population into two separate populations the predicted response rate would allow comparison of enlisted members and officers to determine if there were any significant differences between the two populations. Additionally, demographic measures in the survey allowed comparisons of those having command/supervisory authority over those using USAF microcomputers to those who did not have that authority. The sample was drawn from the ATLAS personnel data base at USAF MPC by Air Force Institute of Technology personnel. By surveying all Air Force personnel versus just those required to use computers on the job (an unisolateable population), the survey encountered a theoretically risky population--those who choose to use micros while not necessarily being fully aware of Air Force policies concerning software copyright infringement. The survey provides a clear picture of the overall understanding of the software piracy program. Had the survey been limited to a sample of people in career specialties with a high likelihood of job-required computer use, it could still have tapped some non-users. More importantly, it may have biased the sample in

one of two possible ways: a) they could be less prone to piracy because of greater familiarity with policy, b) they could be more prone to piracy because of easy access and greater skill. Additionally, limiting the population to computer users only would have limited external validity (generalizability to people in other career specialties) while missing a potentially high-risk group (those who use computers personally, but not on the job, and yet have access to Government systems).

Survey Instrument. The survey instrument for this thesis was based on a compilation of ideas/questions from five similar surveys that had been administered to civilian organizations (2; 3; 38; 39; 41). These surveys assessed issues such as company anti-piracy policies and the attitudes and perceptions of computer users concerning software piracy issues. In addition to questions from the civilian surveys, Air Force specific questions and unique demographic factors of Air Force personnel were solicited in the survey. A copy of the survey instrument is included in Appendix C.

The survey questions were answered according to the respondent's opinion of software piracy issues using a five-point Likert scale. In addition to the Likert scale questions, there were also some "Yes/No" questions to determine the respondent's overall knowledge of copyright issues and their relationships to computer software. A concluding open

ended question was included to allow the respondents to express any opinions not previously addressed as well as allow room for suggestions for the Air Force's anti-piracy program.

Overall, the survey provided information regarding the respondent's opinions and knowledge of the software piracy issue. Upon completion of the survey, the data was then compiled for statistical analysis, using the SAS statistical package (49).

Validity and Reliability of Survey. Validity of the survey was accomplished two-fold. External validity was maintained through using a methodology, i.e., the survey, that had been used previously to measure similar attitudinal questions concerning software piracy. The cross-sectional population encountered by the survey provided additional external validity to the method. Internal validity came from a pre-sample survey of ten AFIT students/personnel to ensure the quality of the survey instrument. Additionally, the survey was reviewed by survey specialists at AFIT to ensure its adequacy and accuracy.

Three reliability checks were used in the methodology. MPC's formula for determining sampling size provide a 90%, +/- 10%, reliability factor that interpreted means that there is a 90% probability, +/- 10%, that the sample is a true representation of the population. The results of the demographics, including time in service and Air Force

Specialty Codes suggests that a good cross-section of Air Force personnel was intersected and as such, the reliability of the survey appears to have been strengthened. The final reliability check came from using a Cronbach coefficient alpha to determine the reliability of the survey with regard to the ability of the instrument to answer the investigative questions. The coefficient can range from 0 - 1, with 1 being the best. Anything above .5 suggests reliability within the acceptable range. The larger the number of questions used to scale an investigative question, the more likely the alpha is to be close to 1. The test was run separately for each population and the results are presented in Table 2.

Table 2. Cronbach Alpha Coefficients

<u>Investigative Question</u>	<u>Officers</u>	<u>Enlisted</u>
2	.8289	.8589
3	.7335	.6584
4	.7559	.5805
5	.5963	.6739
6	.5217	.5363
7	.7397	.6276

The relatively low alpha score for question #6 is attributed to the fact that only three of the survey questions were used to scale this investigative question. Parts of the literature review were further used to answer this question, thereby strengthening the reliability of the

question. Aside from question #6, the other alphas all suggest a strong and reliable instrument.

### Statistical Procedures

In order to run higher order and parametric statistics, several assumptions had to be made concerning the data. These assumptions include independent sampling, normal population, and equal variance between the subpopulations. Additionally, it was assumed that the distance between the points on the Likert scale were equal.

Statistical procedures focused on frequency distributions. Paired t-test procedures were used to determine statistical differences between enlisted and officer responses and also between commander/supervisor and non-commander/supervisor responses. Correlation coefficients were also calculated to determine relationships between the responses to the survey questions and the demographics gathered with the survey. (Prior to running the correlations, the values of the "Yes/No" answered demographics were reversed so that the "Yes" response would be scored a two, and a "No" response would be scored a one. This was done to eliminate confusion brought on by negative correlations that intuitively should appear to be positive.)

A level of significance of  $\alpha = .05$  was set for determining significant differences of means using standard t-tests as well as determining significant correlations between answers and demographics.

### Summary

This chapter outlined the procedures used to complete the research process. The use of this methodology answered the research problem and the seven investigative questions proposed in the introduction. The comparative analysis demonstrates whether or not the Air Force is sufficiently trying to prevent software piracy on its microcomputers. The survey illustrates whether or not the Air Force's efforts are paying off through the prevention of software piracy in the workcenter. The results of the analysis and the survey are presented in the following chapter.

#### IV. RESULTS AND DISCUSSION

##### Overview

This chapter begins with a brief summary of the results for each investigative question and then goes into more detail with each of the answers. Since the first investigative question was answered solely from the literature review, the findings are presented before any of the survey findings. Following the results of the first investigative question, an overview of the survey demographics is presented. The results of the remaining six investigative questions are then presented in detail. The chapter is concluded with a summary of the written comments received from the survey along with a few concluding comments.

##### Summary of Results

The research methodology has successfully answered the seven investigative questions outlined in the first chapter. With regard to investigative question #1, which looked at whether the Air Force is meeting the software industry's minimal criteria for an anti-piracy program, the Air Force is only marginally meeting the policy end of the program. Enforcement of those policies falls short of the full strength allowed by the policies.

In response to investigative question #2, Air Force personnel understand the United States copyright law, Air Force regulations/policies governing software piracy, and to



a lesser extent, software licensing agreements. The area of least understanding is what software can and cannot be placed on Air Force microcomputers and what the penalties are for violating copyright laws. While there are statistically significant differences between some of the responses of enlisted and officers, those differences do not reflect a wide divergence in opinion.

Investigative question #3 was answered with less than half of Air Force personnel perceiving software piracy not to be a problem on Air Force microcomputers. On the other hand, 28.4 percent of the officers and 19.8 percent of the enlisted personnel perceive it to be a problem. Officers tend to see the problem being greater than the enlisted respondents. Enlistees, however, feel that the Air Force is aggressively attempting to stop software piracy and feel more strongly that pirates are apt to be caught. Correlations of the responses to demographics suggest that efforts to stop software piracy should be concentrated with those having the power to stop the problem, i.e., commanders/supervisors, those assigned responsibility for a microcomputer, and those using the systems most frequently.

Investigative question #4 looked at commanders'/supervisors' attitudes and compared them to those without authority over microcomputer users. Almost half of the questions had statistically significant differences between those with authority and their subordinates. Commanders and supervisors understand software piracy issues better than those

without authority. Those in authority also tend to view the software piracy problem as being greater than do those without authority over microcomputer users. Those in authority also reported more frequently to have had a superior or someone else condone or recommend the usage of pirated software.

The strongest results from the survey come in answering investigative question #5. Two survey questions really sum it up best. Question 33 shows that only 6.7 percent of the officers and 9.6 percent of the enlisted feel they can justify software piracy. Question 30 indicates that no commanders or supervisors find it necessary to use pirated software to accomplish their unit's mission.

The results of investigative question #6 suggest that the Air Force is not aggressively trying to prevent illegal software copying and inspecting computers to detect pirated software. Users feel that they are not adequately informed about regulations/policies governing software piracy. Additionally, the literature review shows that marginal regulations and policies exist concerning software piracy, but that they are not enforced to the fullest possibility allowed.

Overall, one might conclude from investigative question #7 that the respondents feel that piracy exists and that the guilty will not be caught, but their impressions are not based on personal experience. They are not sure about the effectiveness of the Air Force program or even that piracy

is a problem. The one thing that the respondents are sure of is that they are personally free of blame.

#### Results of Literature Review in Answering Investigative

#### Question #1: What is the Status of Current Air Force Anti-Piracy Policies and How Do They Compare to the Standards of ADAPSO and the Rest of the Software Industry's Suggested Minimum Standards?

The literature review clearly brought to bear that the Government as a whole, the Department of Defense (DoD), and the Department of the Air Force all have regulations, policies, and guidelines prohibiting the violation of the United States copyright law with regard to computer software. Both the Federal Acquisition Regulation (FAR) and the DoD supplement to the FAR (DFAR) clearly respect the rights of copyright owners when their software is acquired for use on Government computers (24:Part 27.104(g)). The Air Force has at least four regulations which specifically prohibit its users from violating copyrights, and specifically copyrights as they pertain to computer software (15; 13; 16; 14). In addition to the Air Force regulations, several of the major commands have supplemented those regulations with additional guidance with regard to software piracy (17; 18; 19; 20; 21; 22).

All of the major command inspector generals, and small computer centers were contacted for additional material that might be applicable to this thesis. Additionally, the Air

Force Office of Special Investigations, the Judge Advocate General, and other offices with responsibility for small computers and software acquisition/protection were contacted for input. Most of the offices contacted referred the author to the material already cited. Most suggested that their individual offices did not have any additional written guidelines or policies (1; 9; 28; 32; 40). Aside from these organizations, no lower level organizations were contacted for information regarding their software piracy policies. It should be noted, however, that almost 60 percent of the officers and 49 percent of the enlisted personnel responding to the survey knew that their units had specific policies concerning software piracy. The majority of the remaining respondents didn't seem to know one way or the other whether their units had specific policies.

Having looked at the literature of the government, DoD, and the Air Force, it is clear that these organizations have a policy against software piracy. The remaining questions are just how well do these policies meet the suggested minimums of the software industry, and how effective are they?

Software Industry Guidelines. A brief review of the guidelines presented by ADAPSO and the software industry is appropriate at this time as they are the basis for measuring the appropriateness of the Air Force's efforts in preventing software piracy from occurring on its microcomputer assets.

The proposed guidelines are that a program should include 1) the monitoring of software and which machines the software is assigned to, 2) spot checking employees, 3) making software piracy grounds for dismissal, 4) developing an employee education program, 5) involving management in the problem, and 6) obtaining a signed acknowledgement from the employee of his awareness of the law (8:44). Each of these recommendations is looked at individually to determine if the Air Force is meeting the prescribed criteria.

1) The Monitoring of Software and Which Machines the Software is Assigned To. AFR 205-16, Computer Security Policy, outlines the procedures required for conducting a risk analysis which, among other things, includes assigning an individual who is responsible for monitoring software (13). Outside of this regulation, there are no other regulations at this level or above that specifically mention the monitoring of software. However, some of the major commands have added this as a requirement in their supplements to Air Force regulations (17; 18; 19; 20; 21; 22).

While the major commands have made an effort to make the monitoring of software an element of their piracy prevention programs, the Air Force as a whole has not clearly made this an important part of their program. The Air Force is marginally meeting this specific criterion.

2) Spot Checking Employees. Spot checking of employees to determine software piracy problems is almost

unheard of in the Air Force. In numerous conversations with several of the Air Force's inspector generals (IG), it was determined that this type of inspection was rarely conducted. Almost all inspections are prior notice inspections, and most IGs confided that this gave the user ample opportunity to remove any illegal software from their systems. Only one of the major commands has specifically included no notice inspections within their program (19:6).

It is evident that, at this time, the Air Force and most of the major commands do not conduct no notice inspections of their microcomputer resources. As such, the Air Force is failing to meet this criterion of the software industry's recommendations.

### 3) Making Software Piracy Grounds for Dismissal.

Violation of software copyright laws could potentially lead to an offender being discharged from the Air Force. Violation of AFR 205-16, Computer Security Policy, is punishable under the Uniform Code of Military Justice (UCMJ) (13:1). Under UCMJ Article 92 an individual can receive not only fines and confinement for violation of the copyright law (as explained in AFR 205-16), but the individual could be dishonorably discharged from the Air Force (44:IV-28).

Through the numerous contacts with offices already cited, no documented cases of software piracy were noted, nor had there been any reports of prosecution of software piracy incidents within the Air Force (1; 9; 28; 32; 40).

(This is not to say that there weren't any, as most of the IGs pointed out that had there been any such cases, the reports would in all likelihood be non-releasable.) Even in confidential interviews it was suggested that the Air Force has not documented or prosecuted any cases of software piracy in at least the past two or three years. On the grounds of anonymity, one inspector general suggested that in his major command there had been several incidences of software piracy at various units. The only case involving any type of discipline involved an individual who was copying government owned software and taking it home for use on his home computer. The discipline was handled administratively, and the specific punishment was not divulged. It was also pointed out that during unit inspections, if an organization failed in the area of software piracy prevention, those in charge of the program were generally replaced.

While it is clear that the Air Force has a policy that allows for the dismissal of an individual involved with software piracy, the strictest implementation of that policy has not taken place. The Air Force gets a passing mark for meeting this criterion, but has apparently failed to take the strongest possible action allowed under the policy.

4) Developing an Employee Education Program. The Air Force under AFR 205-16 recognizes the importance of training its employees with regard to copyright law and

software piracy prevention. The regulation stipulates that training and awareness are critical for all computer users. It also makes clear that training is to include prohibition of fraud, waste, and abuse as well as the penalties for the violation of this regulation. Initial training is to be conducted at Basic Military Training School and through all of the various officer accession programs (13). A few of the major commands have further instituted policy guidelines within their regulations that require the educating of computer users concerning copyright infringement (18; 20; 21; 22). Whether or not this training is being conducted was not determined.

Since it was not determined whether or not this training is occurring, the Air Force gets a passing mark for having training as part of its policy.

5) Involving Management in the Problem. Once again, AFR 205-16 takes the lead in meeting this criterion. The regulation requires involvement from commanders and management when considering the use of privately owned software on government computers (13:8). However, it fails to go any further on the matter. Military Airlift Command's supplement involves management in conducting the no notice inspections (19:6). Other command supplements also specifically outline some of management's responsibility in preventing software piracy (18; 20; 22).



Just how extensively management should be involved with curtailing software piracy was never determined. However, it appears that at least the major commands are making an effort to ensure this involvement. As a whole, however, the Air Force appears to be only marginally meeting this recommended criterion.

6) Obtaining a Signed Acknowledgement From the Employee of His Awareness of the Law. Nowhere in the literature review was it found that this was an Air Force requirement. Personal experience of the author suggests that some risk analysis at the local unit level might require this, but Air Force wide, and even at the command level, there is no such requirement. For this criterion, the Air Force gets a failing mark.

Overall Score. While the score for each category is simply the author's subjective opinion, it should be clear that the Air Force as a whole is not doing too well at meeting the software industry's recommended criteria. Only criterion four received a solid passing mark. Both criteria one and five were found to be marginal, and two and six were clearly failures. Criterion three received mixed marks of passing for having policy, but an apparent failure in implementing the full strength of the policy. At best, it could be said that the Air Force is marginally meeting the software industry's criteria. The major commands, however, seem to be doing a bit better. Recommendations for improving the

Air Force's score in meeting these criteria will be presented in the next chapter.

#### Overview of Survey Demographics

The survey was completed in April 1990, and any returns received after April 30th were ignored in the analysis. Of the 125 surveys sent out to enlisted personnel, 74 were returned and all but one were usable (a return rate of 59.2 percent). Officers returned 78 of the surveys of which all but three were usable (a return rate of 62.4 percent). Those surveys which were rejected had only part of the survey completed or the respondent used answers outside of the range of the designated scale.

Table 3 provides the various Air Force specialty codes (AFSC) of those enlisted personnel responding to the survey along with the number of respondents within each AFSC. The large number of 45XXX respondents is a result of that career field, which is aircraft maintenance, being the largest enlisted career field in the Air Force. Table 4 provides the same information for the officers. "No AFSC" indicates the number of respondents not providing their AFSC with the survey.

Figure 1 and Figure 2 help to illustrate how well the sample captured the time in service demographics. For enlisted personnel, there were 15 respondents with 0 - 4 years, 28 with 5 - 9 years, 17 with 10 - 14 years, 7 with 15 - 19 years, 4 with 20 - 24 years, and 2 with more than 25

Table 3. Distribution of Enlisted AFSCs (n = 73)

AFSC	FREQ	AFSC	FREQ
10XXX	1	60XXX	1
11XXX	1	63XXX	1
13XXX	1	64XXX	3
20XXX	1	70XXX	3
27XXX	1	73XXX	1
30XXX	5	79XXX	1
41XXX	2	81XXX	3
45XXX	18	90XXX	1
46XXX	3	91XXX	1
49XXX	7	95XXX	1
55XXX	2	NO AFSC	12
57XXX	3		

Table 4. Distribution of Officer AFSCs (n = 75)

AFSC	FREQ	AFSC	FREQ
00XX	3	27XX	1
09XX	1	28XX	5
10XX	4	40XX	3
11XX	3	49XX	4
12XX	2	55XX	1
13XX	3	67XX	1
14XX	5	70XX	2
15XX	3	80XX	1
17XX	4	89XX	2
18XX	1	93XX	1
20XX	1	94XX	1
22XX	4	95XX	2
25XX	3	97XX	2
26XX	2	NO AFSC	10

years of total active military service. On the officer side, there were 21, 17, 16, 11, 8, and respondents in each category respectively.

The third demographic category determined whether the respondent had ever used a USAF owned microcomputer during their career. Some 59 (80.8 percent) enlisted and 70 (93.3

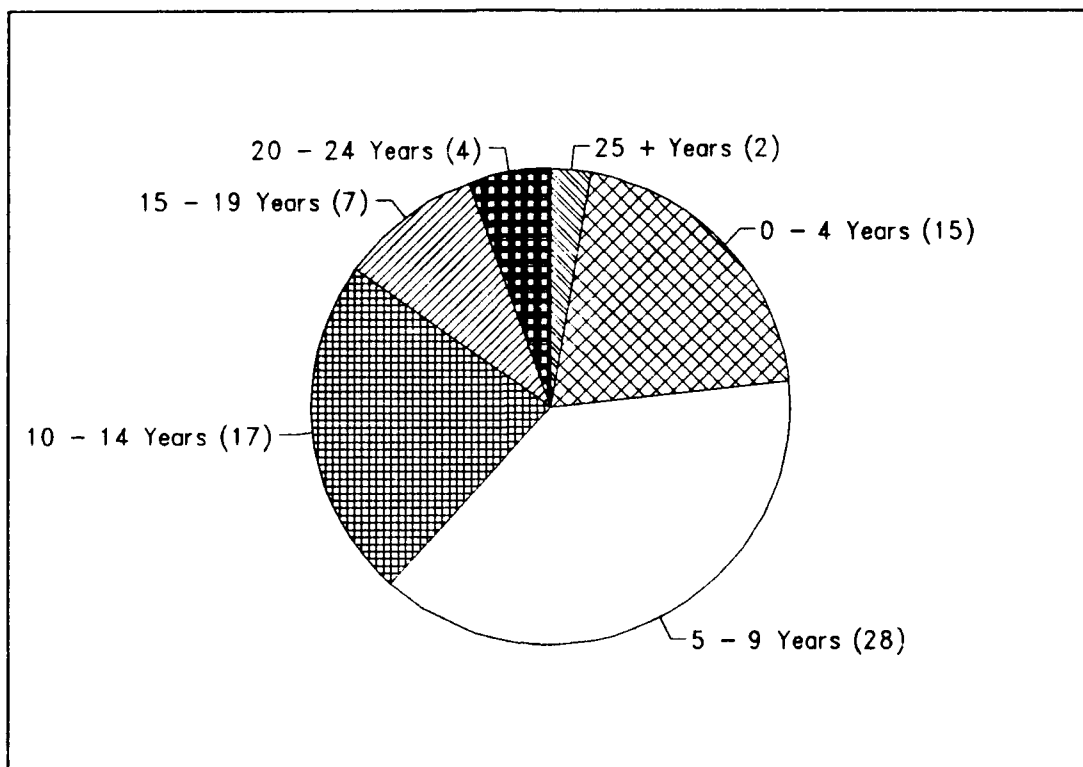


Figure 1. Total Years Active Military Service - Enlisted

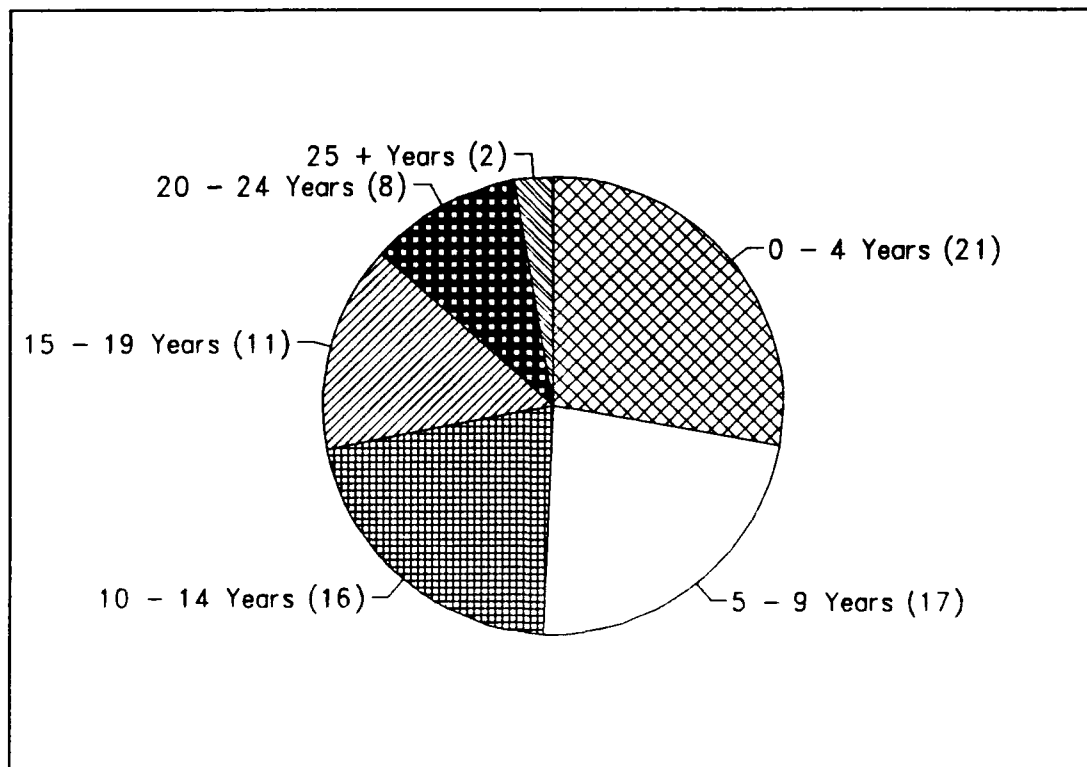


Figure 2. Total Years Active Military Service - Officers

percent) officers responded that they had used USAF microcomputers at least once during their Air Force careers.

Figure 3 and Figure 4 show these users to be more than just one time users. Only one enlisted and three officers claiming computer usage use computers less than yearly.

Types of microcomputer usage are illustrated in Figure 5 and Figure 6, clearly illustrating the fact that wordprocessing is still the number one usage of microcomputers in the Air Force with data base management and presentation graphics finishing second and third respectively.

While computer usage appears to be high amongst Air Force personnel, the number actually assigned responsibility for the computers is much lower. Only 21 (40.0 percent) of the enlisted and 25 (33.3 percent) of the officer respondents were actually assigned responsibility for a microcomputer. Responsibility was defined as control of who uses the computer and what software is placed on the hard drive.

The final demographic gathered by the survey was the number of respondents having command or supervisory authority over other microcomputer users. There were 20 (27.4 percent) of the enlisted respondents and 24 (32.0 percent) of the officers that had the defined authority.

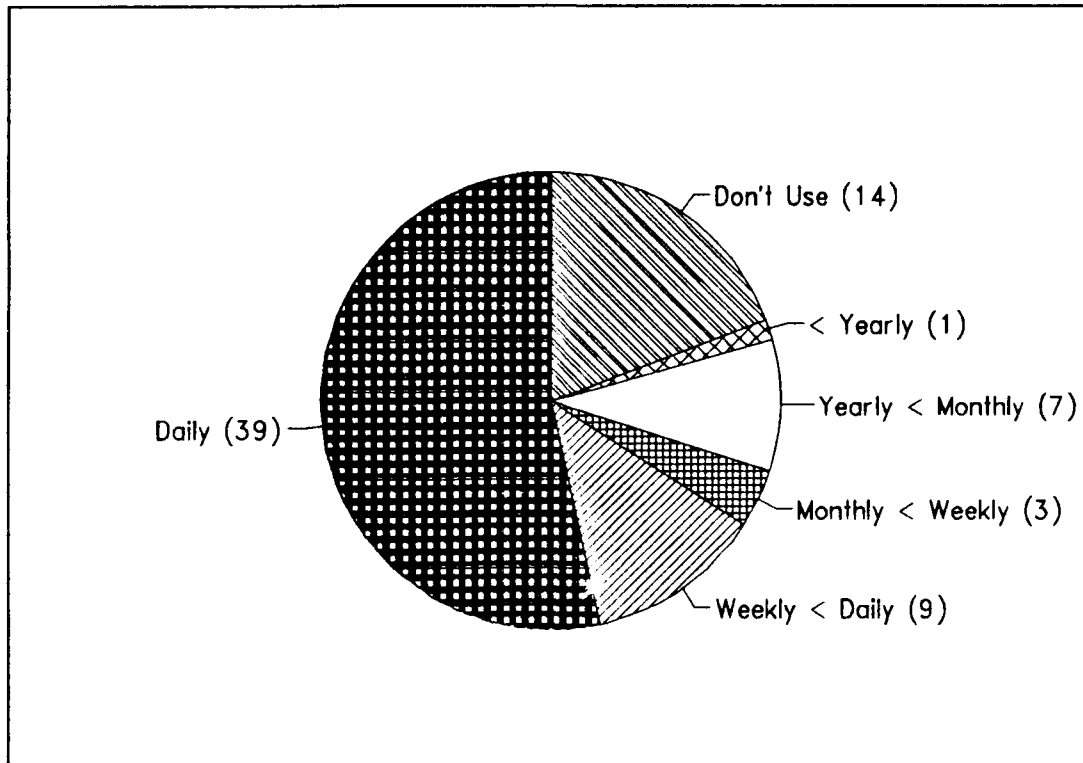


Figure 3. Frequency of Computer Usage - Enlisted

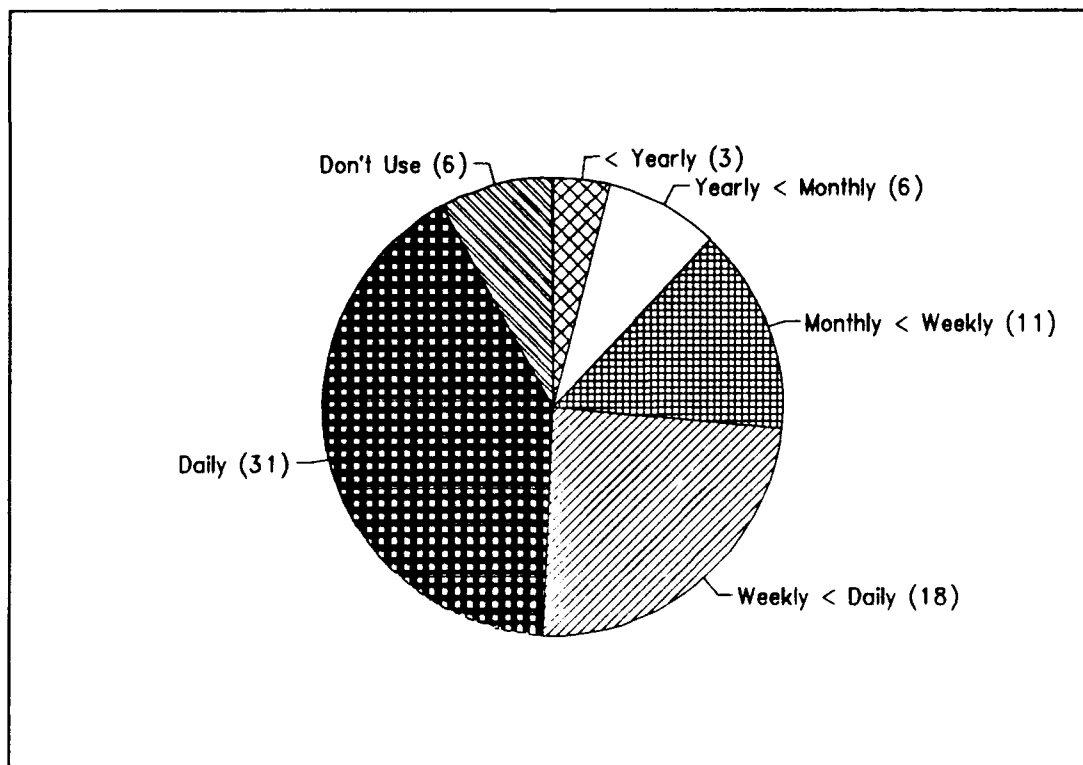


Figure 4. Frequency of Computer Usage - Officers

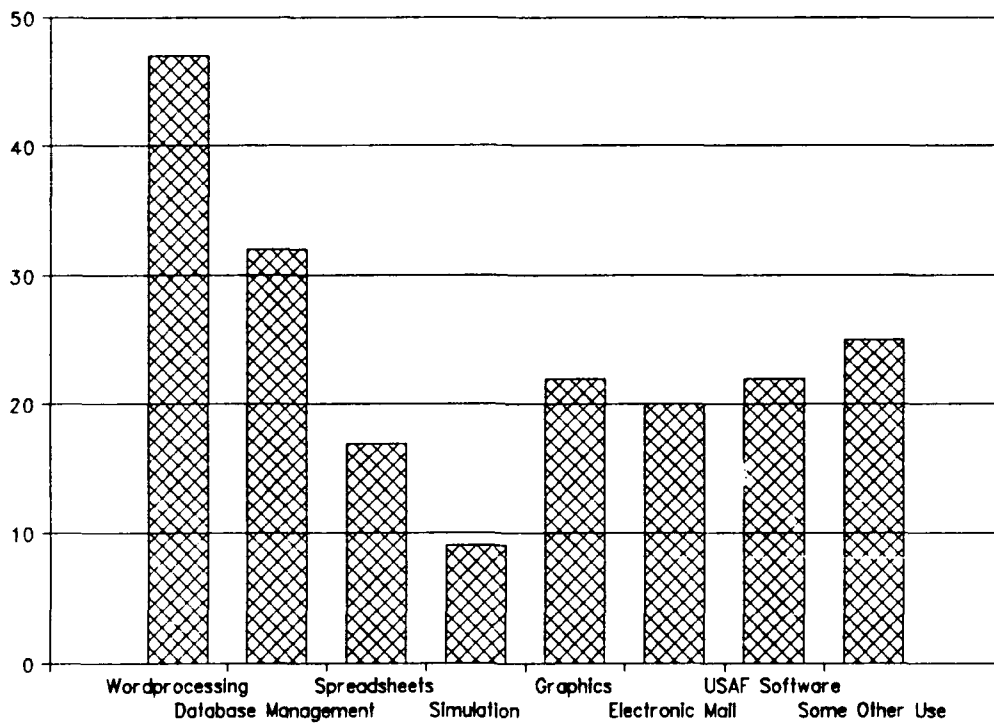


Figure 5. Types of Microcomputer Usage - Enlisted

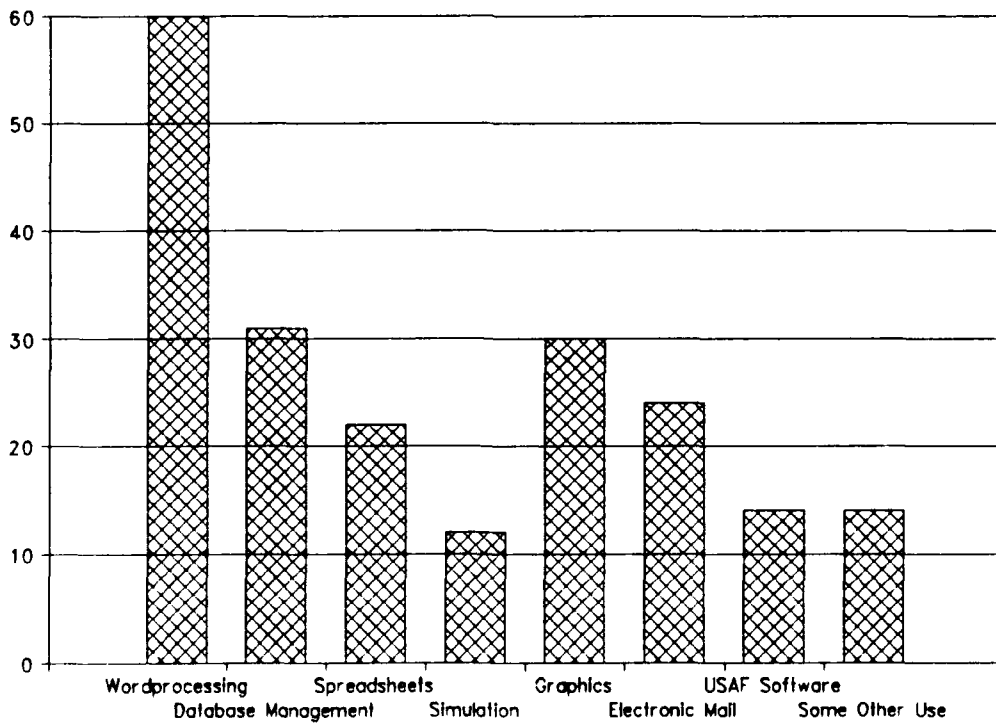


Figure 6. Types of Microcomputer Usage - Officers

Survey Results: Investigative Question #2, How Well Do Air Force Personnel Understand the United States Copyright Law, Software Licensing Agreements, and Air Force Anti-Piracy Regulations?

Investigative question #2 used the following questions from the survey to determine the level of understanding of Air Force personnel with regard to the specific items within the investigative question.

8. I understand the United States copyright law.
9. I understand what software license agreements are.
10. I know what software piracy is.
11. The United States Air Force has formal regulations/policies covering illegal software copying by its members.
12. My unit has formal regulations/policies covering illegal software copying by members of my unit.
13. I understand what software can and cannot be used on an Air Force microcomputer.
17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.
18. I know the potential penalties for violating the U.S. copyright law on Air Force computers.
19. It is legal to make multiple copies of a single software package without obtaining a site license as long as it is done for the Air Force's benefit on Air Force computers.



20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.
21. It is ethical to make multiple copies of a single software package without a site license in order to save the Air Force money.
22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.

Table 5 and Table 6 provide the results to these questions. More specific details are available in Appendix D.

The data indicate that the respondents understand the copyright law, software licensing agreements, and Air Force policies moderately well. The survey questions used to answer the investigative question were designed to be preferably answered in the "Agree - Strongly Agree" area of the Likert scale except for questions 19, 20, and 21 which were designed to be answered in the opposite direction. On the whole, an average of 67.0 percent of the officers and 53.5 percent of the enlisted personnel responded in the affirmative to the survey questions. (Averages were determined by adding the percentages of each response which appeared on the appropriate side of the "Not Sure" response. For example, all of the "Agree" and "Strongly Agree" responses' percentages were added together except for questions 19, 20, and 21. Since these questions were designed to be answered opposite to the rest of the questions, their

Table 5. Officer Responses to Survey Questions for Investigative Question #2

?#	n	S/Dis	Dis	Not Sure	Agr	S/Agr	Mean
8	75	.013	.107	.173	.493	.213	3.79
9	75	.053	.107	.147	.480	.213	3.69
10	75	.013	.000	.027	.600	.360	4.29
11	75	.000	.013	.067	.533	.387	4.29
12	74	.041	.068	.297	.365	.230	3.68
13	75	.053	.173	.320	.307	.147	3.32
17	75	.080	.307	.213	.347	.053	2.99
18	75	.093	.253	.267	.307	.080	3.03
19	75	.227	.387	.333	.040	.013	2.23
20	75	.240	.400	.293	.053	.013	2.20
21	75	.333	.493	.160	.000	.013	1.87
22	75	.027	.080	.053	.467	.373	4.08

Table 6. Enlisted Responses to Survey Questions for Investigative Question #2

?#	n	S/Dis	Dis	Not Sure	Agr	S/Agr	Mean
8	73	.027	.027	.260	.493	.192	3.79
9	73	.068	.068	.397	.288	.178	3.44
10	73	.041	.014	.219	.425	.301	3.93
11	72	.000	.028	.278	.375	.319	3.99
12	73	.041	.027	.438	.315	.178	3.56
13	73	.041	.041	.384	.329	.205	3.62
17	72	.083	.153	.375	.347	.042	3.11
18	73	.041	.068	.452	.329	.110	3.40
19	72	.153	.236	.486	.111	.014	2.60
20	73	.205	.274	.466	.041	.014	2.38
21	73	.205	.274	.411	.068	.041	2.47
22	73	.055	.082	.219	.342	.301	3.75

"Disagree" and "Strongly Disagree" responses were added to the total. The average was arrived at by taking the summation of these percentages and dividing the number by the number of questions (in this case 12). This procedure is used throughout the paper.) On average only 13.4 percent of the officers and 10.0 percent of the enlisted responded

negatively to the survey questions. The remainder of the respondents were "Not Sure" in their responses.

Enlisted responses were generally weighted either in the desired directions or with the "Not Sure" response. However, on question 17 nearly a quarter of the respondents disagreed that users are adequately informed about policies. The remainder of the questions had a very low percentage (less than 15 percent) of the respondents answering in a negative direction. While the enlisted responses to questions 8 and 10 suggest that the respondents understand what software piracy and the copyright law are (68.5 and 72.6 percent respectively agreeing), their responses to questions 18, 19, 20, and 21 suggest that less than 50 percent of the respondents clearly understand the application of the law with regard to software piracy and the severity of the penalties for failure to abide by the law. Enlisted personnel, while feeling confident in their understanding of software piracy and copyright law (as shown by their responses to questions 8 and 10), are less sure of software licensing agreements. A final area of concern brought to light by the enlisted personnel's responses to the survey comes from the responses to question 12. Less than 50 percent of the respondents were aware of their units having regulations or policies concerning software piracy and nearly 44 percent of the respondents were not sure.

The responses suggest that individual units need to educate their people more effectively concerning software

piracy policies and copyright laws. This education should focus on helping the computer user to understand more clearly what software can and cannot be placed on an Air Force microcomputer along with penalties for violating these policies.

Like the enlisted personnel, the officers responding to the survey did not clearly feel that Air Force personnel are adequately informed about policies and regulations governing software piracy. Only 40 percent of the officers actually believed users to be adequately informed. In response to question 13, less than 50 percent of the officers felt they understood what software could be placed on an Air Force computer. However, their responses to questions 19, 20, 21, and 22 (61.4, 64.0, 82.6, and 84.0 percent respectively in the favorable direction) suggest that they understand the issue more clearly than they themselves believe. Officer responses to question 18 suggests that while officers may understand copyright laws (see questions 8, 9, and 10), they are not aware of the potentially severe penalties that exist for violating the law.

Comparing the means between the enlisted and officers at a level of significance of  $\alpha = .05$ , five of the questions were found to have significant differences: 10, 11, 18, 19, and 21. None of the questions had means on opposite sides of the "Not Sure" response. The difference was simply in the strength of agreeing or disagreeing. A quick look at the data suggests that one of the main differences in the

means is a result of enlisted personnel more frequently marking "Not Sure" as their response to the question. In addition to the effect of the "Not Sure" responses, there are also other aspects of the answers worth noting. Officers responding to question 10 clearly understand what software piracy is (96.0 percent agreeing) while less than three-fourths of the enlisted personnel claim an understanding of the subject. Officers appear to be less aware of the potential penalties for software piracy than do the enlisted respondents (34.6 and 10.9 percent respectively disagreeing to the statement that they understand the potential penalties). As already mentioned in the individual analysis to the questions, enlisted personnel do not clearly understand what software can and cannot be placed on Air Force microcomputers (more so than the officers respondents). This point is further illustrated by the difference in the responses to question 21. Nearly 11 percent of the enlisted personnel felt that it was ethical to illegally copy software in order to save the Air Force money where as less than 2 percent of the officers felt likewise. These differences would suggest that enlisted personnel are more in need of education as to what software can and cannot be placed on an Air Force microcomputer and that officers should be educated more along the lines of what the penalties are for violating copyright laws. Specifics for the t-test comparison of the means are in Appendix D.

All of the questions have significant ( $\alpha = .05$ ) correlations with various demographic factors. Direction of correlations are based on the desired response to the question. "Yes/No" answers were correlated with "No" = 1 and "Yes" = 2 and "Enlisted/Officer" responses were given the values of 1 and 2 respectively. The specific details of these correlations can be found in Appendix E.

Survey questions 9, 10, 13, and 19 are correlated with five or more of the seven demographics. These questions primarily tend to relate to understanding of software piracy in general as opposed to knowing Air Force policy. Use of microcomputers or responsibility for a micro seems to be significantly correlated with such general knowledge. Years of military service and whether or not an individual has command/supervisory authority are the two demographics with the greatest number of questions with which they are correlated (11 and 10 out of 12 respectively).

The correlations indicate that those in the Air Force with the greatest amount of time-in-service and those with command authority have a better understanding of copyright laws, licensing agreements, and regulations governing software piracy. As such, if the Air Force wants to improve its efforts to prevent software piracy, then the focus for education should be with first-term enlistees and new officers. This is not to say that continuing education for career members should be ignored, but that the weakest segment of the population surveyed is the younger members of

the Air Force. Also, since it appears that commanders and supervisors have a greater understanding of the issues at hand, then they should make a more concerted effort to pass their knowledge on to their subordinates while continuing to improve their own knowledge and understanding of software piracy issues.

Summary of Results to Investigative Question #2. Air Force personnel understand the United States copyright law, Air Force regulations/policies governing software piracy, and to a lesser degree, software licensing agreements. However, while the respondents claimed a general knowledge, the application of that knowledge was found to be questionable. There are statistically significant differences between some of the responses of enlisted and officers. Significant positive correlations exist between responses and time-in-service and whether or not the respondent has command/supervisory authority over microcomputer users. This suggests that emphasis on training efforts should be greater for the younger airmen and new officers and that the subject of training should be what software can and cannot be placed on Air Force microcomputers along with the penalties for violating copyright laws and Air Force software piracy regulations and policies.

Survey Results: Investigative Question #3, To What Extent  
Do Air Force Personnel Perceive Software Piracy as a Problem  
on USAF Microcomputers?

Investigative question #3 used the following questions from the survey to determine the perception of Air Force personnel as to whether or not they consider software piracy to be a problem on USAF microcomputers.

14. The Air Force aggressively tries to prevent illegal software copying on its microcomputers.
15. The Air Force is successful at preventing software piracy from occurring on its microcomputers.
17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.
23. Software piracy does not occur on USAF microcomputers.
25. I am not aware of any pirated software on USAF owned microcomputers.
26. Software piracy is a problem on Air Force microcomputers.
28. The availability of legally acquired software is adequate for my needs when using Air Force microcomputers.
29. At this time, the software on the computer(s) assigned to me for my use has all been obtained legally.
30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.



31. To the best of my knowledge, I have never used pirated software on Air Force microcomputers.
32. In the past, software piracy was justified on USAF computers.
34. Individuals involved with software piracy on USAF computers are not very likely to get caught.
35. Have you ever heard a superior condone unauthorized software copying?
36. Has anyone ever suggested that you make an unauthorized copy of copy protected software on a USAF micro-computer?
37. Due to circumstances beyond your control, have you ever knowingly used pirated software on an Air Force computer to accomplish your assigned duties?

Table 7 and Table 8 provide the results for these questions. More specific details are available in Appendix D.

The data suggests that less than one-half of both the officers and enlisted personnel perceive software piracy not to be a problem on Air Force microcomputers. All of the questions except for question 26, 30, 32, and 34 were designed to be answered "Agree" or "Strongly Agree" or "No" if the respondent did not perceive there to be a problem. The desired response for the exceptions was either "Disagree" or "Strongly Disagree." On average only 43.9 and 44.9 percent of the officers and enlisted respectively responded to the Likert scale questions in the desired direction. However 87 and 85.2 percent of the officers and

enlisted respectively answered the "Yes/No" questions in the affirmative or desired direction.

Table 7. Officer Responses to Survey Questions for Investigative Question #3

?#	n	S/Dis(Y)	Dis(N)	Not Sure	Agr	S/Agr	Mean
14	75	.053	.240	.373	.253	.080	3.07
15	75	.093	.333	.507	.053	.013	2.56
17	75	.080	.307	.213	.347	.053	2.99
23	75	.307	.453	.160	.067	.013	2.03
25	74	.068	.176	.243	.378	.135	3.34
26	75	.027	.080	.600	.213	.080	3.24
28	65	.046	.138	.062	.538	.215	3.74
29	49	.061	.041	.082	.469	.347	4.00
30	33	.485	.394	.121	.000	.000	1.64
31	64	.031	.156	.203	.344	.266	3.66
32	75	.227	.320	.413	.040	.000	2.27
34	75	.013	.147	.347	.387	.107	3.43
35	69	.101	.899				1.90
36	69	.159	.841				1.84
37	69	.130	.870				1.87

Table 8. Enlisted Responses to Survey Questions for Investigative Question #3

?#	n	S/Dis(Y)	Dis(N)	Not Sure	Agr	S/Agr	Mean
14	73	.000	.151	.370	.356	.123	3.45
15	73	.082	.178	.575	.137	.027	2.85
17	72	.083	.153	.375	.347	.042	3.11
23	73	.205	.288	.452	.027	.027	2.38
25	73	.055	.110	.233	.411	.192	3.58
26	73	.014	.082	.644	.164	.096	3.25
28	55	.036	.127	.145	.455	.236	3.73
29	41	.073	.049	.122	.341	.415	3.98
30	36	.389	.528	.083	.000	.000	1.69
31	58	.069	.086	.190	.310	.345	3.78
32	73	.192	.164	.589	.027	.027	2.53
34	73	.082	.151	.452	.247	.068	3.07
35	63	.190	.810				1.81
36	63	.143	.857				1.86
37	63	.111	.889				1.89

On the other hand, an average of 28.4 percent of the officers and 19.8 percent of the enlisted personnel answered

the Likert scale question in the negatively desired direction, suggesting a perception of there being a problem with software piracy on Air Force computers. Those who were "Not Sure" in their responses came up an average of 27.7 and 35.3 percent of the officer and enlisted responses.

Comparing the means between the enlisted and officers at an alpha level of .05 suggests some results that differ from the above mentioned averages. Four of the 15 questions showed significant differences between the two populations: 14, 15, 23, and 34. The responses to question 14 suggest that only one-third of the officers surveyed feel that the Air Force is aggressively trying to prevent software piracy while 47.9 percent of the enlisted personnel feel that an aggressive effort is being made. While the enlisted feel that the Air Force is aggressively trying to stop software piracy, their responses to question 15 indicate that only 16.4 of the respondents felt that the Air Force is successful in its efforts. Even though the officers were split with their opinions as to the Air Force's aggressiveness at preventing software piracy, 42.6 percent indicated that they do not feel that the Air Force is successful at stopping software piracy on its computers. The officers significantly differed with the enlisted's opinions in that the officers felt that the Air Force was much less successful at preventing piracy from occurring on its systems. While very few of the officers and enlisted personnel (8.0 and 5.4 percent respectively) felt that software piracy did not

occur on Air Force microcomputers (question 23), there was a divergence of opinion with disagreement to the question. Over three-fourths of the officers and less than one-half of the enlisted personnel indicated, through their disagreement to the question, that they felt that software piracy occurs on Air Force microcomputers. In response to question 34, nearly 50 percent of the officers agreed to the statement that software pirates on Air Force computers are not very likely to get caught while only 31.5 percent of the enlisted personnel felt similarly. From the questions with significant differences and the overall averages of the responses, it appears that officers perceive software piracy to be a greater problem on Air Force computers than do the enlisted respondents. Specifics for the t-test comparison of the means are in Appendix D.

The survey questions used to answer investigative question #3 do not appear to have a lot of correlation to demographics even though some significant correlations do exist ( $\alpha = .05$ ). Correlations were set up as mentioned in the results for investigative question #2.

Significant correlations of enlisted and officer responses exist for questions 14, 15, 23, and 34. If one recalls, these are the same questions that had significantly different means when the t-test was applied.

There is a significant correlation between years of service and questions 17, 26, and 32. This would suggest that those with longer time-in-service feel that while users

are well informed about policies and regulations concerning piracy there continues to be a problem with software piracy. Interestingly enough, those with longer time-in-service, however, do not feel that piracy was justified in the past while those with less time-in-service seem to think that piracy was justified in the past.

Having ever used a USAF microcomputer is only significantly correlated with question 23 (negative correlation). This suggests that those who have never used a USAF microcomputer do not feel that piracy occurs on Air Force systems. On the other hand, the who have used USAF micros feel that piracy does occur. One should be careful before making too much of this correlation, however, since the number of respondents who had never used an Air Force microcomputer is very small (14 enlisted and 5 officers).

Those who use Air Force computers the most seem to be more aware of pirated software than those who use the machines less frequently based on the negative correlation of question 25 with frequency of use. Also those who use computers more frequently reported higher incidences of superiors condoning software piracy, having had others recommend the unauthorized copying of software, and the use of pirated software to accomplish their assigned duties (see specific correlations to questions 35, 36, and 37).

There is a significant correlation between those who have a computer assigned to them and their beliefs that the Air Force is not successfully preventing software piracy

(question 15) and that software piracy is a problem on Air Force computers (question 26). While there is a significant correlation between those assigned computers and question 29 it should be pointed out that only those assigned microcomputers should have responded to the question, therefore the correlation is in question.

The most common demographic having any type of significant correlation is the supervisor/commander demographic (six of the 15 questions). Commanders and supervisors feel more strongly that users are informed about existing regulations and policies concerning software piracy (question 17). Yet, those same commanders also feel more strongly that the Air Force is not successfully preventing software piracy and that the problem persists (question 15, 23, and 26). Commanders and supervisors also reported more frequently that they themselves have had superiors and others condone the illegal copying and use of software on Air Force equipment. Perceptions of and involvement with software piracy appear to be more correlated with officers, those with high frequency of computer usage, and those with supervisory or command authority over computer users. An exerted effort should be made to ensure that those with the power to significantly reduce software piracy, i.e., commanders/supervisors, those assigned computers, and those who use them the most frequently, are themselves striving to prevent piracy from occurring. Overall education concerning software piracy, as previously mentioned, should be emphasized

more to the junior members of the Air force. Specific details of the correlations can be found in Appendix E.

Summary of Results to Investigative Question #3. On an average, less than half of Air Force personnel perceive software piracy not to be a problem on Air Force microcomputers. On the other hand, 28.4 percent of the officers and 19.8 percent of the enlisted personnel perceive it to be a problem. There are statistically significant differences of perception between the two populations surveyed with regards to questions 14, 15, 23, and 34. Enlisted personnel more frequently felt that the Air Force was aggressively attempting to stop software piracy while officers felt that those efforts were not being successful and that offenders were not very likely to be caught. Significant correlations exist between many of the survey questions. Especially noteworthy are the correlations of frequency of usage, assignment of a computer, and supervisory/command authority to the survey questions. Efforts to prevent software piracy should therefore be applied to all segments of the Air Force community but should be emphasized to those in the power to stop software piracy, i.e. commanders/supervisors, high frequency users, and those assigned responsibility for the systems. Education should be targeted to the junior enlistees and officers as previously mentioned.

Survey Results: Investigative Question #4, What Are the Attitudes of Supervisors/Commanders Concerning Software Copyright Infringement?

Investigative question #4 compared the responses to the following questions based on whether or not the respondent answered that he was a commander/supervisor of microcomputer users in question #7 of the survey.

12. My unit has formal regulations/policies covering illegal software copying by members of my unit.
17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.
19. It is legal to make multiple copies of a single software package without obtaining a site license as long as it is done for the Air Force's benefit on Air Force computers.
20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.
21. It is ethical to make multiple copies of a single software without a site license in order to save the Air Force money.
22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.
23. Software piracy does not occur on USAF microcomputers.
24. Under no circumstance would I use pirated software on an Air Force microcomputer.



25. I am not aware of any pirated software on USAF owned microcomputers.
26. Software piracy is a problem on Air Force micro-computers
27. While I would not be involved with copying Air Force owned software, I personally have no problem with using pirated software on my home computer.
28. The availability of legally acquired software is adequate for my needs when using Air Force micro-computers.
30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.
32. In the past, software piracy was justified on USAF computers.
33. Today, I can find no justification for the Air Force or its members to violate the U.S. copyright law by unauthorized copying of commercial software.
34. Individuals involved with software piracy on USAF computers are not very likely to get caught.
35. Have you ever heard a superior condone unauthorized software copying?
36. Has anyone ever suggested that you make an unauthorized copy of copy protected software on a USAF micro-computer?

37. Due to circumstances beyond your control, have you ever knowingly used pirated software on an Air Force computer to accomplish your assigned duties?

Specific frequencies were not calculated for each response. Instead, the mean of commanders/supervisors and non-commanders/supervisors were calculated and t-test analyses were conducted to determine any significant differences (alpha = .05). Table 9 provides the result of this analysis, and additional data is available in Appendix F.

Table 9. Mean Scores of Commanders/Supervisors and Non-Commanders/Supervisors (\* statistically significant differences)

Question	Com/Sup	Non-Com/Sup	p-Value
12	3.82	3.53	0.1132
17	3.36	2.91	0.0165 *
19	2.02	2.57	0.0008 *
20	2.05	2.39	0.0332 *
21	1.89	2.28	0.0218 *
22	4.14	3.83	0.0421 *
23	1.84	2.36	0.0023 *
24	3.65	3.81	0.4287
25	3.34	3.50	0.4148
26	3.52	3.12	0.0152 *
27	2.88	2.90	0.9359
28	3.60	3.80	0.3422
30	1.62	1.73	0.4637
32	2.18	2.49	0.0567
33	4.00	3.88	0.4544
34	3.27	3.24	0.8544
35	1.73	1.91	0.0329 *
36	1.73	1.89	0.0457 *
37	1.81	1.91	0.1949

Commanders and supervisors significantly differ in their answers in 9 of the 19 questions used to answer this investigative question. Only question #17 shows a

difference between commanders/supervisors agreeing while their counterparts seem to disagree very slightly. In other words, commanders/supervisors tend to feel that computer users are adequately informed with regard to policies and regulations governing software piracy. On the other hand, non-commanders/supervisors have a slight tendency to feel that users are not adequately informed. This may be a result of the fact that commanders/supervisors themselves are more informed about copyright laws, licensing agreements, and regulations concerning software piracy (see the answer to investigative question #2).

There are some important conclusions that can be drawn from the above information. Questions 19, 20, 21, and 22 all involve knowing what is legal or ethical versus what isn't. In all four cases, commanders/supervisors tend to show a greater understanding of what is and isn't legal/ethical.

Questions 23 and 26 look at whether or not the respondent feels that software piracy is a problem on USAF micro-computers. In both cases, it appears that commanders/supervisors perceive there to be more of a problem than do their subordinates.

Questions 35 and 36 look at whether or not a respondent's superior has condoned software piracy or if anyone has ever suggested to the respondent that he use pirated software. Commanders and supervisors responded "Yes" more frequently than did those without command/supervisory

authority indicating they are personally aware of incidents of a problem, thereby reinforcing the results of questions 23 and 26.

Correlations of supervisors/commanders and non-commanders/supervisors are available in Appendix E. Specific significance of the correlations are detailed where appropriate in the other investigative questions.

#### Summary of Results to Investigative Question #4.

Almost half of the investigative questions demonstrated a significant difference in the responses of those with authority over microcomputers and their subordinates. Commanders and supervisors appear to be more educated with regards to software piracy issues. They also tend to feel that there is a greater problem with software piracy than do their subordinates which is reinforced by their having personal experience with others condoning or recommending the use of pirated software.

#### Survey Results: Investigative Question #5, Under What Circumstances Do USAF Personnel Feel That Software Copyright/License Infringement is Justified and/or Legal?

The following survey questions were used to answer investigative question #5 in determining what Air Force personnel considered as justification for infringing on copyright and license agreements.

19. It is legal to make multiple copies of a single software package without obtaining a site license as long as it is done for the Air Force's benefit on Air Force computers.
20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.
21. It is ethical to make multiple copies of a single software without a site license in order to save the Air Force money.
22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.
24. Under no circumstance would I use pirated software on an Air Force microcomputer.
27. While I would not be involved with copying Air Force owned software, I personally have no problem with using pirated software on my home computer.
28. The availability of legally acquired software is adequate for my needs when using Air Force microcomputers.
30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.
33. Today, I can find no justification for the Air Force or its members to violate the U.S. copyright law by unauthorized copying of commercial software.

Table 10 and Table 11 provide the results of these questions. More specific details are available in Appendix D. (The low number of responses to questions 27, 28, and 30 are a result of special qualifiers built into the question which allowed "Not Applicable" responses.)

Table 10. Officer Responses to Survey Questions for Investigative Question #5

?#	n	S/Dis	Dis	Not Sure	Agr	S/Agr	Mean
19	75	.227	.387	.333	.040	.013	2.23
20	75	.240	.400	.293	.053	.013	2.20
21	75	.333	.493	.160	.000	.013	1.87
22	75	.027	.080	.053	.467	.373	4.08
24	73	.055	.151	.164	.397	.233	3.60
27	36	.167	.306	.194	.222	.111	2.81
28	65	.046	.138	.062	.538	.215	3.74
30	33	.485	.394	.121	.000	.000	1.64
33	75	.000	.067	.200	.493	.240	3.91

Table 11. Enlisted Responses to Survey Questions for Investigative Question #5

?#	n	S/Dis	Dis	Not Sure	Agr	S/Agr	Mean
19	72	.153	.236	.486	.111	.014	2.60
20	73	.205	.274	.466	.041	.014	2.38
21	73	.205	.274	.411	.068	.041	2.47
22	73	.055	.082	.219	.342	.301	3.75
24	73	.000	.096	.205	.384	.315	3.92
27	29	.172	.207	.241	.207	.172	3.00
28	55	.036	.127	.145	.455	.236	3.73
30	36	.389	.528	.083	.000	.000	1.69
33	73	.014	.082	.219	.342	.342	3.92

There is strong evidence from the above data that Air Force personnel can find little justification for infringing on copyrights and licensing agreements. Questions 22, 24, 28, and 33 were designed to be answered in the "Strongly

Agree - Agree" categories to reflect no justification for software piracy. Questions 19, 20, 21, 27, and 30 were designed to be answered "Strongly Disagree - Disagree" if the respondent could find no justification for copyright/license infringement. The average officer response rate was 71 percent in the desired direction and the enlisted responses were 59.6 percent in the affirmative, or in other words, unable to find a justification for software piracy. On average, only 11.4 percent of the officers and 12.9 percent of the enlisted personnel could find any justification for software piracy.

Only two of the questions, 19 and 21, had significant differences in their means. Both of these differences were explained in the results to investigative question #2. To summarize, however, officers tend to better understand what software can and cannot be placed on Air Force microcomputers and under what circumstances.

Using the correlation method described in the results of investigative question #2, questions 19, 20, 21 and 22 show some significant correlations ( $\alpha = .05$ ) while the rest of the questions show no significant correlations at all. These questions are significantly correlated to time-in-service and commander/supervisor demographics. The questions deal with what is legal/ethical with regard to copying software. The correlations suggest that those with more time-in-service and those with command/supervisory authority over microcomputer users have a greater

understanding of what is and isn't legal and/or ethical. More specifically, questions 19, 20, and 21 identify circumstances under which there is a potential benefit to the Air Force in pirating software. Under those circumstances, enlisted people, junior members, light users, and non-supervisors tend to be more willing to pirate software. This would once again suggest that training needs to be emphasized for the junior members of the Air Force. The issue, however, may need more than just education to resolve the problem. Management involvement may play a key factor (recall that this is one of the software industry's recommendations to an affective anti-piracy program) in solving this problem. Management must be involved with computer users and set the appropriate example, making it clear that not even a benefit to the Air Force justifies software piracy. Specific details of correlations for the four correlated questions have previously been discussed and additional details are available in Appendix E.

Summary of Results to Investigative Question #5. The strongest results from the survey come in answering investigative question #5. Two survey questions really sum it up best. Question 33 shows that only 6.7 percent of the officers and 9.6 percent of the enlisted feel they can justify software piracy. Question 30 indicates that no commanders or supervisors find it necessary to use pirated software to accomplish their unit's mission. While there might be an



existing problem as already suggested in previous investigative questions, it appears that there is little or no justification for Air Force members to be involved in software piracy on Air Force resources. To correct those areas where members feel that there is a justification for software piracy, education and management involvement are critical to resolving the problem.

Survey Results: Investigative Question #6, What Efforts Can/Are Commanders, Supervisors, and the Air Force as a Whole Use(ing) to Prevent Software Piracy from Occurring on USAF Resources?

Investigative question #6 used the following questions from the survey to determine what methods, if any, are being used to prevent software piracy from occurring on its microcomputers.

14. The Air Force aggressively tries to prevent illegal software copying on its microcomputers.
16. The Air Force actively inspects microcomputers to detect illegal software.
17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.

Table 12 and Table 13 provide the results to these questions. More specific details are available in Appendix D.

The above questions were used to determine if, from the perception of the respondents, the Air Force is making an effort to prevent software piracy from occurring. If so,

then the responses would have been reflected in "Agree - Strongly Agree" answers. Enlisted personnel tend to feel

Table 12. Officer Responses to Survey Questions for Investigative Question #6

?#	n	S/Dis	Dis	Not Sure	Agr	S/Agr	Mean
14	75	.053	.240	.373	.253	.080	3.07
16	75	.053	.280	.480	.160	.027	2.83
17	75	.080	.307	.213	.347	.053	2.99

Table 13. Enlisted Responses to Survey Questions for Investigative Question #6

?#	n	S/Dis	Dis	Not Sure	Agr	S/Agr	Mean
14	73	.000	.151	.370	.356	.123	3.45
16	73	.055	.137	.534	.219	.055	3.08
17	72	.083	.153	.375	.347	.042	3.11

that more of an effort is being made than do the officers. On average, 38.1 percent of the enlisted responses felt that an effort was being made while 30.7 percent of the officers felt the same way. On the other hand, an average of 33.8 percent of the officers felt that an effort was not being made while only 19.3 percent of the enlisted personnel agreed. There was a large number (42.6 and 35.5 percent enlisted/officers respectively) of "Not Sure" responses.

Only question 14 showed a significant difference between the means of the two populations. 48 percent of the enlisted personnel and only 33 percent of the officers believe that the Air Force is aggressively trying to prevent illegal software copying on its microcomputers. Additional

insight concerning the differences were brought out under the results to investigative question #3. Specific details of the differences in the means are available in Appendix D.

These three questions had very little correlation with the demographics. Question 14 is correlated to the enlisted/officer demographic, reinforcing the difference in the populations already cited. Question 17 is correlated to the years in service and the supervisor/commander demographics. As previously mentioned, this suggests that those who are more informed about the issues at hand (see investigative question #2) feel that everyone else is equally well informed. As a result, those with greater time-in-service and command/supervisory experience need to share their knowledge with subordinates so that their perceptions might more clearly reflect reality. Specific details of how the correlations were conducted are available in the results of investigative question #2 and the complete results are available in Appendix E.

While the survey answered part of investigative question #6, additional insight comes from the literature review. In brief, the literature review suggested that the Air Force has several regulations/policy statements that should prevent software piracy from occurring on its computer resources, but it is apparent from the survey result that those regulations/policies are not being enforced to the full strength allowed by the policies.

Summary of Results to Investigative Question #6. These results suggest that enlisted personnel feel that the Air Force is making an effort to stop software piracy. The officers tend to differ somewhat from that opinion. Additionally, supervisors/commanders feel more than do the enlistees that users are not adequately informed concerning regulations and policies governing software piracy. If the Air Force wants its policies and regulations to prevent software piracy, it is going to have to make a greater effort in educating users (especially junior members) about regulations/policies governing software piracy. The literature review showed that regulations and policies exist concerning software piracy, but that their enforcement often falls short of the full strength allowed by those policies. Overall, a greater effort to prevent software piracy should be demonstrated by the Air Force. Also, in the summary of the written comments provided later in this chapter, some suggested methods to reduce software piracy are presented.

Survey Results: Investigative Question #7, Do USAF Personnel Believe That Current Regulations and Guidelines Concerning Software Piracy Adequately Prevent Piracy From Occurring on Air Force Microcomputers?

Investigative question #7 used the following questions from the survey to determine if Air Force personnel feel that existing regulations/policies concerning copyright infringement are fulfilling their purpose.

15. The Air force is successful at preventing software piracy from occurring on its microcomputers.
16. The Air Force actively inspects microcomputers to detect illegal software.
23. Software piracy does not occur on USAF microcomputers.
25. I am not aware of any pirated software on USAF owned microcomputers.
26. Software piracy is a problem on Air Force micro-computers
29. At this time, the software on the computer(s) assigned to me for my use has all been obtained legally.
31. To the best of my knowledge, I have never used pirated software on Air Force microcomputers.
34. Individuals involved with software piracy on USAF computers are not very likely to get caught.
35. Have you ever heard a superior condone unauthorized software copying?

Table 14 and Table 15 provide the results to the questions. Details to the responses are available in Appendix D.

Respondents were fairly evenly split in trying to decide whether or not the Air Force is successful at preventing software piracy from occurring on its microcomputers, with a high number of "Not Sure" (an average of 32.8 and 40.0 percent officers and enlisted respectively). All of the survey questions designed to answer this investigative question, except questions 26 and 34, were set up so

Table 14. Officer Responses to Survey Questions for Investigative Question #7

?#	n	S/Dis (Y)	Dis (N)	Not Sure	Agr	S/Agr	Mean
15	75	.093	.333	.507	.053	.013	2.56
16	75	.053	.280	.480	.160	.027	2.83
23	75	.307	.453	.160	.067	.013	2.03
25	74	.068	.176	.243	.378	.135	3.34
26	75	.027	.080	.600	.213	.080	3.24
29	49	.061	.041	.082	.469	.347	4.00
31	64	.031	.156	.203	.344	.266	3.66
34	75	.013	.147	.347	.387	.107	3.43
35	69	.101	.899				1.90

Table 15. Enlisted Responses to Survey Questions for Investigative Question #7

?#	n	S/Dis (Y)	Dis (N)	Not Sure	Agr	S/Agr	Mean
15	73	.082	.178	.575	.137	.027	2.85
16	73	.055	.137	.534	.219	.055	3.08
23	73	.205	.288	.452	.027	.027	2.38
25	73	.055	.110	.233	.411	.192	3.58
26	73	.014	.082	.644	.164	.096	3.25
29	41	.073	.049	.122	.341	.415	3.98
31	58	.069	.086	.190	.310	.345	3.78
34	73	.082	.151	.452	.247	.068	3.07
35	63	.111	.889				1.89

that "Agree - Strongly Agree" responses would indicate that the Air Force was being successful in its endeavors to prevent software piracy. Questions 26 and 34 were designed to be answered "Disagree - Strongly Disagree" to reflect the same point. By averaging the responses, 31.7 percent of the officers and 35.4 percent of the enlisted indicated that they felt the Air Force's program was successful. On the other hand, 35.4 percent of the officers and 24.4 percent of the enlisted felt that current regulations and guidelines were not successfully preventing software piracy from

occurring on USAF computers. Averaging the answers may obscure more detailed findings, making it difficult to say from the survey whether or not the Air Force is successfully preventing software piracy on its systems.

Looking at the individual questions even leaves the answer to the investigative question up in the air. For example, question 23 suggests that the respondents feel that software piracy occurs on Air Force computers (76 percent officer and 49.3 percent enlisted). However, question 29 indicates that the respondents are not the guilty parties (81.6 percent officers and 75.6 percent enlisted claiming their computers are free from pirated software). Question 26 demonstrates that 60.0 percent of the officers and 64.4 percent of the enlisted personnel are not sure if piracy is a problem on Air Force computers. Many of the respondents are not sure if the Air Force successfully enforces its anti-piracy regulations (question 15) or if the Air Force routinely inspects computers for pirated software (question 16). Yet, not knowing the above facts did not keep the respondents from indicating that they do not feel that guilty parties are very likely to be caught (question 34) (61.0 percent of the officers and 65.5 percent of the enlisted). Finally, while both parties feel that software piracy occurs (see above figures), 51.3 percent of the officers and 60.3 percent of the enlistees indicated that they were not personally aware of pirated software on Air Force

microcomputers (question 25). They also claim no personal piracy on Air Force computers (question 31) and have not had supervisors condone piracy (question 35). Once again, the results are so mixed it is not clear if the Air Force's efforts are truly preventing software piracy from occurring on its microcomputers.

Comparing the individual questions shows that three of the questions, 15, 23, and 34, have means that significantly differ between the two populations ( $\alpha = .05$ ). These questions have had their differences explained previously in the results of investigative question #3. In summary, officers did not feel that the Air Force's anti-piracy efforts were effective. Over three-fourths of the officers felt that piracy occurs on Air Force computers compared to less than 50 percent of the enlistees. Enlisted responses suggested that they feel that pirates are more likely to be caught than do the officers responding to the survey. Specific information concerning t-test results are available in Appendix D.

Several significant patterns can be determined from the correlations. Most of these have been previously mentioned in the answers to previous investigative questions. To review, officer-enlisted differences are reinforced. Frequent users are more likely to have encountered problems and are personally aware of pirated software and have heard superiors condone software piracy. Officers and supervisors are also more likely to perceive a problem and are also more



likely to have heard superiors condone the use of pirated software. It appears that while there are some additional significant correlations between the answers and various demographic categories, these correlations do not provide any clearly beneficial information. Specific details of the correlations are available in Appendix E.

#### Summary of Results to Investigative Question #7.

Overall, one might conclude that the respondents feel that piracy exists and that the guilty will not be caught, but their impressions are not based on personal experience. They are not sure about the effectiveness of the Air Force program or even that piracy is a problem. The one thing that the respondents are sure of is that they are personally free of blame.

#### Survey Results: Summary of Written Comments.

Eighteen of the respondents added additional comments to their surveys. Many of those adding comments appear, from the tone of their comments, to have very strong opinions concerning the subject matter. Of those providing written comment, approximately one-third of the respondents indicated that they feel that software piracy is a problem on Air Force computers. Two of the eighteen respondents stressed that while they felt it was a problem in the past, the word seems to be getting out as to what can and cannot be used on a microcomputer. Several causes of software piracy were suggested: 1) Lack of education or

understanding by users and superiors; 2) Requirements from higher echelons (i.e., require information be passed along on disk in a format provided by software not legally owned by the unit); 3) Necessity to meet mission requirements; 4) Lack of funds; 5) Lack of standardization (see #2 above) and; 6) Difficult acquisition process. Others stressed the difficulty in catching violators. Finally, several individuals passed on successes that their units are having or methods that they feel would, if implemented, prevent piracy from occurring in their units. These suggestions or methods include improved training at tech schools, ensure adequate funding for software, routinely briefing what software can and cannot be used on Air Force microcomputers, conducting routine inspections along with spot checks for illegal software accompanied by follow-up inspections, tell people what's correct/incorrect and why, education to the user level in the form of an interactive program taking no longer than 15 min at an eighth grade reading level, standardize software where possible, and finally, provide a deterrent to discourage the use of pirated software. All appropriate written comments are provided in Appendix G for review.

Several of the written comments do not correlate (in the non-statistical sense) very well with the data because these comments appear to come from the vocal few and are not really representative of the whole group. Yet, the written comments do provide some insights as to what might be the cause of the problem, as well as providing solutions that

might help resolve the software piracy issue on Air Force microcomputers.

### Conclusion

While the Air Force has policies and regulations that could amount to a foundation for an anti-piracy program, its enforcement of those regulations and policies falls short of the full strength allowed by the policies as demonstrated in the results of investigative questions 1, 6, and 7. Investigative question #1 indicated marginal regulations and policies with unconfirmed enforcement. Question #6 supports question #1's results in that the respondents did not seem to feel that the Air Force is aggressively attacking the issue. Question #7 suggested that many feel that software piracy is a problem, but that their beliefs are not based on personal experience. It is clear that while the respondents feel that there is a problem, they feel that they are not personally to blame.

Responses to investigative question #2 suggest that personnel understand copyright laws, the regulations and policies that support these laws, and to a lesser extent licensing agreements. Responses to question #5 strongly indicated that Air Force members do not feel there is much justification for violating copyright laws and licensing agreements. However, investigative question #3 suggests that less than 50 percent of the personnel surveyed seem to think that there is not a problem with software piracy.

Comparing commanders and supervisors of microcomputer users to those without said authority showed that commanders and supervisors are more educated than their subordinates concerning software piracy issues. Commanders and supervisors also felt that the software piracy problem was greater than did those without authority over computer users which was supported by the fact that they themselves also had more personal experience with supervisors or others condoning or recommending the use of pirated software.

Having come up with the above conclusions, the next chapter will provide some suggestions to overcoming the weaknesses of the Air Force's efforts to prevent software piracy. In addition, the next chapter will provide some suggested follow-on research that might strengthen the findings of this paper.

## V. Conclusions and Recommendations

### Overview

This chapter summarizes the findings of this thesis and provides some recommendations on how the United States Air Force might improve its efforts to prevent software piracy. It also suggests some of the implications that this paper holds for the Air Force. Additionally, the chapter provides some suggestions regarding future research that might be conducted in the area of software piracy prevention.

### Summary of Findings and Recommendations

None of the seven investigative questions were answered as positively as they should have been if the Air Force were actively trying to prevent software piracy from occurring on its microcomputers. The results of each question can be improved with some modifications and improvements to the Air Force's existing regulations and policies.

Investigative question #1 reviewed the Air Force's existing policies and tried to determine if those policies were being enforced. It was determined that the policies are only marginal and enforcement of those policies falls short of the full strength allowed by the policies.

Investigative #2 indicated that Air Force personnel feel that they understand copyright laws, licensing agreements (to a lesser extent), and the current regulations governing software piracy. The interpretation of those laws

and policies appears to be lacking in that the enlisted responses suggested that the respondents did not clearly understand what software can and cannot be loaded onto an Air Force microcomputer.

The extent of software piracy was not determined. However, investigative question #3 suggested that less than half of those surveyed perceived software piracy not to be a problem, while 28.4 percent of the officers and 19.8 percent of the enlisted personnel perceive it to be a problem. If this is a reflection of reality, then there must be some level of copyright infringement occurring on USAF resources. In fact, if the Air Force is similar to American business, then pirated software could account for between 22 and 50 percent of all software on Air Force microcomputers.

In response to investigative question #4, commanders and supervisors of microcomputer users varied significantly from those without authority in almost 50 percent of the answers. Commanders and supervisors understand copyright issues more clearly, perceive the piracy problem to be greater, and have more frequently had others suggest to them or condone the use of pirated software than did those without similar authority.

The brightest light came from the responses to investigative question #5. It was here that the respondents to the survey indicated that as a whole, there is no justification in the Air Force for using pirated software. Only one such justification was brought to bear in the written comments of

the survey where one individual simply stated that "mission accomplishment is paramount." However, the survey question dealing explicitly with this matter indicated that commanders and supervisors as a whole do not agree with that comment.

Investigative question #6 indicated that the respondents did not feel that the Air Force is aggressively trying to prevent illegal software copying. The question also suggested that the Air Force is not actively inspecting computers for pirated software and that users do not feel that they are adequately informed concerning regulations and policies governing software piracy.

In answering investigative question #7, the respondents indicated that they feel software piracy exists on Air Force systems, and that those involved in the piracy are not very likely to be caught. As a result, the respondents do not feel that the Air Force is effectively preventing software piracy from occurring on its computers. Most of the respondents were not speaking from personal experience. Clearly, the one point that did come out of the question was that the respondents do not feel that they are personally to blame, but that the problem exists with their contemporaries.

In order to improve the desired responses to this survey, the Air Force needs to make several changes to its existing policies and regulations. Not only do changes need to be made to the regulations, but once the changes are made, they need to be enforced to their fullest extent where

warranted if the Air Force wishes to have microcomputers free from pirated software.

Recommendations for Change. To improve the situation, the Air Force needs to add a few items to their existing policies in order to get them within the guidelines of the software industry. Many of these suggestions are supported by the written comments from the survey. Policies must make it mandatory that software be more tightly controlled and monitored, ensuring that each software package is only used on one machine unless the licensing agreement states otherwise. Each local organization (department or squadron level equivalent) should have a central storage point for master disks. By maintaining a central storage point, the copying of master disks may be more tightly controlled. Software serial numbers should be indexed with the central processing unit's serial numbers so that inspections can easily verify what software is assigned to which system.

Inspections need to include pre-announced as well as random, no-notice spot-checks. While pre-announced inspections are becoming routine, the Air Force as a whole has yet to implement random checking. Several of the inspector generals stated that one of the reasons they find very little pirated software is because users are knowledgeable enough to remove pirated software prior to announced inspections. It is believed that no-notice inspections, conducted by IG teams as well as supervisors and automated data



processing equipment monitors would go a long way in preventing software piracy from occurring (see Appendix G, comments 7, 8, and 9).

Enforcement of the regulations and policies concerning software piracy needs to be accompanied with strict penalties for the parties involved. If this is the situation today, it is not common knowledge. Non-publicizing of names and penalties may be a result of protecting individual privacy; however, penalties could be more publicized, making every effort possible to protect the defendants' privacy. By making judgements more publicized, the judgements will become a deterrent to the problem (see Appendix G, comments 8 and 17).

While education concerning copyright infringement should occur when each member enters the Air Force, the program also needs to be made on-going. The data suggests that it is the junior members of the Air Force that do not clearly understand software copyright issues and regulations. Therefore more emphasis should be made to ensure that computer users understand early on what is and isn't legal to copy and use. Additional training could be added to Basic Training along with the officer accession programs. Education on these issues could also be provided during commander's calls as well as during various training courses. Computer users need to be kept informed of and reminded about copyright laws and licensing agreements. Current understanding of these issues should be made

mandatory for microcomputer users. Prior to receiving authorization to work on USAF microcomputers, the user should receive some type of indoctrination concerning the unit's policies concerning software piracy as well as additional information that might help the user to know what is and is not legal. The Air Force could also go an additional step by producing and distributing visual aids on the subject matter to be posted in computer areas. These visual aids could be simplistic yet provide a recurring reminder to the user that software piracy will not be tolerated on Air Force microcomputers (see Appendix G, comments 2, 7, and 8).

Management needs to become more involved with the problem. While only about 10 percent of the respondents indicated that they had had superiors condone software piracy, the problem seems to exist. Management must set the example as well as being involved in the education of personnel and the enforcement of the policies and regulations (see Appendix G, comments 2, 5, 7, 8, 9, 15, and 18).

Prior to use of any USAF owned microcomputer, it should be made mandatory that users sign some type of a statement such as the one in Appendix A. By making this a requirement, the Air Force and management will stand a greater chance of being relieved of liability should a software vendor seek compensation for a copyright or software license infringement. Computer users should sign this statement annually to ensure that members are being reminded about the importance of the issue.

One method for reducing software piracy would be to standardize various application packages. However, this would have had to occur at the onset of microcomputer acquisition. Today it is too late to even begin considering such an option. Most computer users are comfortable with the programs that they work with. To get those users to change to a standard package for the sake of standardization would be extremely difficult. Additionally, there are also legitimate differences in need that can justify differences in software. For example, engineers tend to need word-processing packages capable of formulae and scientific notation whereas information managers and personnel managers require software that have more user friendly interfaces. Even then, there is still a need for standard formats for "shared" data between the various communities so that data can be combined and submitted to a common higher office. As illustrated, standardization is clearly not the sole answer to solving the software piracy issue (see Appendix G, comments 1, 12, and 17).

By making these additions to its policies and regulations, the Air Force will bring its program into line with the recommended criteria of the software industry. However, implementing the policy alone will not fulfill all of the requirements. The Air Force must also make greater strides in stricter enforcement of these policies.

### Implications to the Air Force

The implications of this thesis to the United States Air Force are wide-spread. As a user of microcomputers and numerous software packages, the Air Force must eliminate liability for itself and its members by ensuring that software piracy does not exist in the Air Force.

As budget cuts make it more difficult to procure the required software, it is essential that members not be tempted to 'beat the system' by using pirated software. Commanders must ensure that they budget adequate funds to meet software requirements. To further eliminate the temptation to pirate software, the Air Force may also need to simplify the software acquisition process. This would make it much simpler for users to acquire the software that they need in a timely manner.

With the implementation of the numerous local area networks (LANS) and wide area networks, the Air Force again will find itself challenged with new issues concerning licensing agreements and copyright law. Developers of these systems must keep current on existing legislation and regulations if they hope to avoid using pirated software. Many of the questions that exist with LANS software are being resolved by the software industry moving toward tailored license agreements for software specifically designed for LANS.

The survey showed that virtually every member of the Air Force is going to use computers to accomplish their

various jobs. From aircraft mechanics to engineers, military personnel are having to become computer literate. Part of that literacy must entail an understanding of copyright laws and licensing agreements. The implications of this thesis five or ten years ago would have applied simply to those in the computer career field. Today, they apply to everyone in the Air Force.

#### Recommendations for Further Research

While this thesis looked at perceptions and attitudes, one area needing the greatest research is to determine to what extent software piracy is actually occurring on Air Force microcomputers. To determine this level, a researcher would need to go out and randomly spot check microcomputers for pirated software. The researcher could use a utility package that detects deleted software to determine if any pirated software had been recently deleted. By determining the extent of the problem, the Air Force, and the specific units involved could tailor their programs to prevent software piracy from occurring.

#### Conclusion

This thesis has shown that while the Air Force has made some in-roads in the prevention of software piracy, there is still much to be done. Through discussions with numerous individuals and in reviewing the written comments received with the survey, it appears that the piracy situation is much better today than it was five or ten years ago.

However, the Air Force is in no position to curtail its anti-piracy efforts. If the Air Force wants to continue making ground on the problem then the changes recommended in this chapter must be implemented. If those changes are made and the regulations and policies strictly enforced, then software piracy should become a thing of the past on Air Force computer systems.

Appendix A: Signed Statement of Acknowledgement

I recognize that:

1. (Company, Organization) licenses the use of its computer software from a variety of outside companies. (Company, Organization) does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.
2. With regard to use on local area networks or on multiple machines, (Company, Organization) employees shall use the software only in accordance with the license agreement.
3. (Company, Organization) employees learning of any misuse of software or related documentation within the company, shall notify their department manager or (Company's. Organization's) legal counsel.
4. (Company, Organization) employees caught making, acquiring or using unauthorized copies of computer software will be disciplined as appropriate under the circumstances.
5. According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of \$50,000 or more, and criminal penalties including fines and imprisonment.

I am aware of the software protection policies of (Company, Organization).

---

Employee Signature

---

Date (43)

Appendix B: Organizations Contacted for Thesis Support

ADAPSO  
Suite 300  
1300 No 17th St  
Arlington, VA 22209

ASSOCIATION FOR COMPUTING MACHINERY  
11 W. 42nd Street, 3rd Floor  
New York, NY 10036

ASSOCIATION OF SYSTEMS MANAGEMENT  
Journal of Systems Management  
24587 Bagley Rd  
Cleveland, OH 44138

BUSINESS  
Georgia State University  
College of Business Administration  
Business Publishing Division  
University Plaza  
Atlanta, GA 30303

CALIFORNIA STATE UNIVERSITY, SACRAMENTO  
Dept of MIS  
6000 J Street  
Sacramento, CA 95819  
Susan L. Solomon  
(916) 278-7129

COLORADO STATE UNIVERSITY  
College of Business  
Computer Information Systems Dept  
Ft Collins, CO 80523  
Susan B. Athey  
303-491-6203

COMPUTER DECISIONS  
Beatech Publishing Co  
Glenpoint Center E  
DeGraw Ave  
Teaneck, NJ 07666

GENERAL ACCOUNTING OFFICE  
Mr Fred Gallegos  
Los Angeles, CA  
213-894-3813



GOVERNMENT COMPUTER NEWS  
P.O. Box 3705  
McLean, VA 22103-9834

MISSISSIPPI STATE UNIVERSITY  
College of Business and Industry  
Mississippi State, MS 39762  
601-325-3928  
JPSHIM@MSSTATE.BITNET

MIS QUARTERLY  
MIS Research Center  
Carlson School of Management  
271 19th Avenue S  
University of Minnesota  
Minneapolis, MN 55455

OLD DOMINION UNIVERSITY  
Norfolk, VA 23529

OR/MS TODAY  
Operations Research Society of America  
428 E. Preston St  
Baltimore, MD 21202

SOFTWARE PUBLISHERS ASSOCIATION  
1101 Connecticut Ave, NW Suite 901  
Wash DC 20036  
(202) 452-1600

WASHBURN UNIVERSITY of TOPEKA  
Topeka, KA 66621

AFOSI  
Bolling AFB, DC 20332-6001

AFCC (SC, IG)  
Scott AFB, IL 62225-6001

AFLC (SC, IG)  
Wright-Patterson AFB, OH 45433-5001

AFSPACECOM (SC, IG)  
Peterson AFB, CO 80914-5000

AFSC (SC, IG)  
Andrews AFB, MD 20334-5000

ATC (SC, IG)  
Randolph AFB, MD 78150-5001

AU  
Maxwell AFB, AL 36112-5001

ESC (SC, IG)  
San Antonio, TX 78243-5000

MAC (SC, IG)  
Scott AFB, IL 62225-5001

SAC (SC, IG)  
Offutt AFB, NE 68113-5001

HQ USAF/IG  
Wash DC 20330-5120

TAC (SC, IG)  
Langley AFB, VA 23665-5001

AF Communications Computer Security Mgmt Office (AFCSMO)  
AFCSC/SR  
San Antonio, TX 78243-5000

HQ USAF/SCT  
Wash DC 20330-5190

AF Communications Systems Doctrine Office (AFCSDO)  
HQ USAF/SCP  
Keesler AFB, MS 39534-6340  
AV 868-3410

HQ USAF/SCPX  
Wash DC 20330-5190

AF Judge Advocate Legal Information Services  
HQ USAF/JAS  
Denver, CO 80279-5000

AF Legal Service Center  
AFLSC  
WASH DC 20330-5120

Appendix C: Computer Software Piracy Survey

USAF Survey Control Number SCN 90-23

INSTRUCTIONS

1. Use the Standard Answer Sheet provided to mark your answers to the questionnaire. YOU DO NOT HAVE TO GIVE YOUR NAME OR SOCIAL SECURITY NUMBER!!
2. In the "School Code" block of the answer sheet, mark the first four digits of your Duty Air Force Specialty Code (DAFSC). NOTE: You must write in the numerals across the top and fill in the corresponding spaces in the columns.
3. Use a number 2 pencil only.
4. Be sure to completely fill in the oval for your answer without going outside the lines. If you change your answer, be sure you erase your original answer completely.
5. Mark only one answer for each question unless otherwise told.
6. After you have completed the questionnaire, please put the Standard Answer Sheet and the questionnaire in the return envelope and place it in your normal outgoing distribution. Please return the survey no later than \_\_\_\_\_

### Computer Software Piracy Survey

Answer all questions that pertain to you as of today (circle or check as appropriate)

1. I am an

A. Enlisted

B. Officer

2. My total years of active military service is (check one)  
(Disregard partial years, i.e. 4 3/4 yrs. will check  
0 - 4 yrs)

A. 0 - 4

D. 15 - 19

B. 5 - 9

E. 20 - 24

C. 10 - 14

F. 25 +

3. I have used an Air Force owned microcomputer (ie. Z-100,  
Z-248, Macintosh, etc.) at least once during my Air  
Force career.

A. Yes

B. No

4. I use Air Force microcomputers

A. Less than once a year

D. At least once a week

B. At least once a year and  
less than once a month

and less than daily

E. Daily

C. At least once a month and  
less than once a week

F. Do not use Air Force  
owned microcomputers

5. I have used Air Force microcomputers for (check all that apply)

A. Wordprocessing

E. Electronic Mail

B. Database Management

F. USAF Software (i.e. RIMS, RAMS,  
PDOS, CAMS, etc.)

C. Spreadsheets

G. Some other use

D. Simulation/Modeling

H. Do not use Air Force owned  
microcomputers

6. I have an Air Force owned microcomputer(s) assigned to me and am  
responsible for who uses it, for what software is placed  
on the hard drive, etc.

A. Yes

B. No

7. I have supervisory/command authority over microcomputer users in my  
organization

A. Yes

B. No

For the following questions, use the following scale:

- | 1                    | 2        | 3        | 4     | 5                 | 6                 |
|----------------------|----------|----------|-------|-------------------|-------------------|
| Strongly<br>Disagree | Disagree | Not sure | Agree | Strongly<br>Agree | Not<br>Applicable |
8. I understand the United States copyright law.
  9. I understand what software license agreements are.
  10. I know what software piracy is.
  11. The United States Air Force has formal regulations/policies covering illegal software copying by its members.
  12. My unit has formal regulations/policies covering illegal software copying by members of my unit.
  13. I clearly understand what software can and cannot be used on an Air Force microcomputer.
  14. The Air Force aggressively tries to prevent illegal software copying on its microcomputers.
  15. The Air Force is successful at preventing software piracy from occurring on its microcomputers.
  16. The Air Force actively inspects microcomputers to detect illegal software.
  17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.
  18. I know the potential penalties for violating the U.S. copyright law on Air Force computers.
  19. It is legal to make multiple copies of a single software package as long as it is done for the Air Force's benefit on Air Force computers.
  20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.
  21. It is ethical to make multiple copies of a single software package in order to save the Air Force money.
  22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.
  23. Software piracy does not occur on USAF microcomputers.
  24. Under no circumstance would I use pirated software on an Air Force microcomputer.

1	2	3	4	5	6
Strongly	Disagree	Not sure	Agree	Strongly	Not
Disagree				Agree	Applicable

25. I am not aware of any pirated software on USAF owned microcomputers.
26. Software piracy is a common problem on Air Force microcomputers.
27. While I would not be involved with copying Air Force owned software, I personally have no problem with copying software on my home computer.
28. The availability of legally acquired software is adequate for my needs when using Air Force microcomputers.
29. At this time, the software on the computer(s) assigned to me has all been obtained legally.
30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.
31. To the best of my knowledge, I have never used pirated software on Air Force microcomputers.
32. In the past, software piracy was justified on USAF computers.
33. Today, I can find no justification for the Air Force or its members to violate the U.S. copyright law by unauthorized copying of commercial software.
34. Individuals involved with software piracy on USAF computers are not very likely to get caught.

Answer the following questions A. Yes or B. No

35. Have you ever heard a superior condone unauthorized software copying

A. Yes B. No

36. Has anyone ever suggested that you make an unauthorized copy of copy protected software on a USAF microcomputer

A. Yes B. No

37. Due to circumstances beyond your control, have you ever used pirated software on an Air Force computer to accomplish your assigned duties?

A. Yes B. No

38. Other Comments (Use the rest of this page and its back if necessary)

Appendix D: Survey Result in Percentages Along With  
p-Values for 2-Sample T-Test of Means  
OFFICER vs ENLISTED

**8. I understand the United States copyright law.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	1.3	2.7	
Disagree	10.7	2.7	
Not Sure	17.3	26.0	
Agree	49.3	49.3	
Strongly Agree	21.3	19.2	
Mean	3.79	3.79	0.9585

**9. I understand what software license agreements are.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	5.3	6.8	
Disagree	10.7	6.8	
Not Sure	14.7	39.7	
Agree	48.0	28.8	
Strongly Agree	21.3	17.8	
Mean	3.69	3.44	0.1551

**10. I know what software piracy is.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	1.3	4.1	
Disagree	0.0	1.4	
Not Sure	2.7	21.9	
Agree	60.0	42.5	
Strongly Agree	36.0	30.1	
Mean	4.29	3.93	0.0093



11. The United States Air Force has formal regulations/  
policies covering illegal software copying by its  
members.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	0.0	0.0	
Disagree	1.3	2.8	
Not Sure	6.7	27.8	
Agree	53.3	37.5	
Strongly Agree	38.7	31.9	
Mean	4.29	3.99	0.0154

12. My unit has formal regulations/policies covering  
illegal software copying by members of my unit.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	4.1	4.1	
Disagree	6.8	2.7	
Not Sure	29.7	43.8	
Agree	36.5	31.5	
Strongly Agree	23.0	17.8	
Mean	3.68	3.56	0.4893

13. I understand what software can and cannot be used on an  
Air Force microcomputer.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	5.3	4.1	
Disagree	17.3	4.1	
Not Sure	32.0	38.4	
Agree	30.7	32.9	
Strongly Agree	14.7	20.5	
Mean	3.32	3.62	0.0867

14. The Air Force aggressively tries to prevent illegal  
software copying on its microcomputers.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	5.3	0.0	
Disagree	24.0	15.1	
Not Sure	37.3	37.0	
Agree	25.3	35.6	
Strongly Agree	8.0	12.3	
Mean	3.07	3.45	0.0159

**15. The Air Force is successful at preventing software piracy from occurring on its microcomputers.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	9.3	8.2	
Disagree	33.3	17.8	
Not Sure	50.7	57.5	
Agree	5.3	13.7	
Strongly Agree	1.3	2.7	
Mean	2.56	2.85	0.0350

**16. The Air Force actively inspects microcomputers to detect illegal software.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	5.3	5.5	
Disagree	28.0	13.7	
Not Sure	48.0	53.4	
Agree	16.0	21.9	
Strongly Agree	2.7	5.5	
Mean	2.83	3.08	0.0784

**17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	8.0	8.3	
Disagree	30.7	15.3	
Not Sure	21.3	37.5	
Agree	34.7	34.7	
Strongly Agree	5.3	4.2	
Mean	2.99	3.11	0.4740

**18. I know the potential penalties for violating the U.S. copyright law on Air Force computers.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	9.3	4.1	
Disagree	25.3	6.8	
Not Sure	26.7	45.2	
Agree	30.7	32.9	
Strongly Agree	8.0	11.0	
Mean	3.03	3.40	0.0305

19. It is legal to make multiple copies of a single software package without obtaining a site license as long as it is done for the Air Force's benefit on Air Force computers.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	22.7	15.3	
Disagree	38.7	23.6	
Not Sure	33.3	48.6	
Agree	4.0	11.1	
Strongly Agree	1.3	1.4	
Mean	2.23	2.60	0.0149

20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	24.0	20.5	
Disagree	40.0	27.4	
Not Sure	29.3	46.6	
Agree	5.3	4.1	
Strongly Agree	1.3	1.4	
Mean	2.20	2.38	0.2225

21. It is ethical to make multiple copies of a single software without a site license in order to save the Air Force money.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	33.3	20.5	
Disagree	49.3	27.4	
Not Sure	16.0	41.1	
Agree	0.0	6.8	
Strongly Agree	1.3	4.1	
Mean	1.87	2.47	0.0001

22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	2.7	5.5	
Disagree	8.0	8.2	
Not Sure	5.3	21.9	
Agree	46.7	34.2	
Strongly Agree	37.3	30.1	
Mean	4.08	3.75	0.0654

23. Software piracy does not occur on USAF microcomputers.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	30.7	20.5	
Disagree	45.3	28.8	
Not Sure	16.0	45.2	
Agree	6.7	2.7	
Strongly Agree	1.3	2.7	
Mean	2.03	2.38	0.0214

24. Under no circumstance would I use pirated software on an Air Force microcomputer.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	5.5	0.0	
Disagree	15.1	9.6	
Not Sure	16.4	20.5	
Agree	39.7	38.4	
Strongly Agree	23.3	31.5	
Mean	3.60	3.92	0.0757

25. I am not aware of any pirated software on USAF owned microcomputers.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	6.8	5.5	
Disagree	17.6	11.0	
Not Sure	24.3	23.3	
Agree	37.8	41.1	
Strongly Agree	13.5	19.2	
Mean	3.34	3.58	0.1963

**26. Software piracy is a problem on Air Force micro-computers**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	2.7	1.4	
Disagree	8.0	8.2	
Not Sure	60.0	64.4	
Agree	21.3	16.4	
Strongly Agree	8.0	9.6	
Mean	3.24	3.25	0.9606

**27. While I would not be involved with copying Air Force owned software, I personally have no problem with using pirated software on my home computer.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	16.7	17.2	
Disagree	30.6	20.7	
Not Sure	19.4	24.1	
Agree	22.2	20.7	
Strongly Agree	11.1	17.2	
Mean	2.81	3.00	0.5568

**28. The availability of legally acquired software is adequate for my needs when using Air Force micro-computers.**

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	4.6	3.6	
Disagree	13.8	12.7	
Not Sure	6.2	14.5	
Agree	53.8	45.5	
Strongly Agree	21.5	23.6	
Mean	3.74	3.73	0.9553

29. At this time, the software on the computer(s) assigned to me for my use has all been obtained legally.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	6.1	7.3	
Disagree	4.1	4.9	
Not Sure	8.2	12.2	
Agree	46.9	34.1	
Strongly Agree	34.7	41.5	
Mean	4.00	3.98	0.9192

30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	48.5	38.9	
Disagree	39.4	52.8	
Not Sure	12.1	8.3	
Agree	0.0	0.0	
Strongly Agree	0.0	0.0	
Mean	1.64	1.69	0.7166

31. To the best of my knowledge, I have never used pirated software on Air Force microcomputers.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	3.1	6.9	
Disagree	15.6	8.6	
Not Sure	20.3	19.0	
Agree	34.4	31.0	
Strongly Agree	26.6	34.5	
Mean	3.66	3.78	0.5742

32. In the past, software piracy was justified on USAF computers.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	22.7	19.2	
Disagree	32.0	16.4	
Not Sure	41.3	58.9	
Agree	4.0	2.7	
Strongly Agree	0.0	2.7	
Mean	2.27	2.53	0.0709

33. Today, I can find no justification for the Air Force or its members to violate the U.S. copyright law by unauthorized copying of commercial software.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	0.0	1.4	
Disagree	6.7	8.2	
Not Sure	20.0	21.9	
Agree	49.3	34.2	
Strongly Agree	24.0	34.2	
Mean	3.91	3.92	0.9419

34. Individuals involved with software piracy on USAF computers are not very likely to get caught.

	OFFICER	ENLISTED	p-VALUE
Strongly Disagree	1.3	8.2	
Disagree	14.7	15.1	
Not Sure	34.7	45.2	
Agree	38.7	24.7	
Strongly Agree	10.7	6.8	
Mean	3.43	3.07	0.0250

35. Have you ever heard a superior condone unauthorized software copying?

	OFFICER	ENLISTED	p-VALUE
Yes	10.1	19.0	
No	89.9	81.0	
Mean	1.90	1.81	0.1528

36. Has anyone ever suggested that you make an unauthorized copy of copy protected software on a USAF micro-computer?

	OFFICER	ENLISTED	p-VALUE
Yes	15.9	14.3	
No	84.1	85.7	
Mean	1.84	1.86	0.7929

37. Due to circumstances beyond your control, have you ever knowingly used pirated software on an Air Force computer to accomplish your assigned duties?

	OFFICER	ENLISTED	p-VALUE
Yes	13.0	11.1	
No	87.0	88.9	
Mean	1.87	1.89	0.7364



Appendix E: Pearson Correlation Coefficients  
p-Values Under Ho:  $\rho = 0$

**8. I understand the United States copyright law.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0043	0.9585
Years of Military Ser.	0.2213	0.0069
Have Used USAF Micro	0.1559	0.0585
Frequency of Use	0.1675	0.0419
Assigned a Micro	0.2028	0.0135
Supervisory/Command	0.3122	0.0001

**9. I understand what software license agreements are.**

	CORRELATION	p-VALUE
Enlisted/Officer	0.1175	0.1551
Years of Military Ser.	0.2738	0.0008
Have Used USAF Micro	0.2565	0.0016
Frequency of Use	0.2884	0.0004
Assigned a Micro	0.3079	0.0001
Supervisory/Command	0.3273	0.0001

**10. I know what software piracy is.**

	CORRELATION	p-VALUE
Enlisted/Officer	0.2147	0.0088
Years of Military Ser.	0.2145	0.0031
Have Used USAF Micro	0.1962	0.0169
Frequency of Use	0.1813	0.0274
Assigned a Micro	0.1684	0.0408
Supervisory/Command	0.2798	0.0006

**11. The United States Air Force has formal regulations/  
policies covering illegal software copying by its  
members.**

	CORRELATION	p-VALUE
Enlisted/Officer	0.2008	0.0147
Years of Military Ser.	0.1847	0.0251
Have Used USAF Micro	0.1512	0.0676
Frequency of Use	0.1382	0.0950
Assigned a Micro	0.1425	0.0851
Supervisory/Command	0.2081	0.0114

**12. My unit has formal regulations/policies covering illegal software copying by members of my unit.**

	CORRELATION	p-VALUE
Enlisted/Officer	0.0575	0.4893
Years of Military Ser.	0.2917	0.0003
Have Used USAF Micro	0.0448	0.5898
Frequency of Use	0.0465	0.5760
Assigned a Micro	0.1409	0.0888
Supervisory/Command	0.1312	0.1132

**13. I understand what software can and cannot be used on an Air Force microcomputer.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1413	0.0867
Years of Military Ser.	0.3538	0.0001
Have Used USAF Micro	0.2476	0.0024
Frequency of Use	0.3082	0.0001
Assigned a Micro	0.3139	0.0001
Supervisory/Command	0.3592	0.0001

**14. The Air Force aggressively tries to prevent illegal software copying on its microcomputers.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1979	0.0159
Years of Military Ser.	0.1464	0.0759
Have Used USAF Micro	-0.0648	0.4341
Frequency of Use	-0.0355	0.6682
Assigned a Micro	-0.1321	0.1094
Supervisory/Command	-0.0197	0.8121

**15. The Air Force is successful at preventing software piracy from occurring on its microcomputers.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1735	0.0350
Years of Military Ser.	-0.1500	0.0689
Have Used USAF Micro	-0.1126	0.1730
Frequency of Use	-0.1527	0.0640
Assigned a Micro	-0.2683	0.0010
Supervisory/Command	-0.2467	0.0025

**16. The Air Force actively inspects microcomputers to detect illegal software.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1451	0.0784
Years of Military Ser.	0.0633	0.4446
Have Used USAF Micro	-0.0436	0.5990
Frequency of Use	0.0003	0.9972
Assigned a Micro	-0.0966	0.2428
Supervisory/Command	-0.1162	0.1596

**17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0595	0.4740
Years of Military Ser.	0.2669	0.0011
Have Used USAF Micro	-0.0624	0.4529
Frequency of Use	-0.0898	0.2792
Assigned a Micro	0.0394	0.6354
Supervisory/Command	0.1976	0.0165

**18. I know the potential penalties for violating the U.S. copyright law on Air Force computers.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1779	0.0305
Years of Military Ser.	0.2098	0.0105
Have Used USAF Micro	0.0190	0.8187
Frequency of Use	0.0475	0.5666
Assigned a Micro	0.2014	0.0141
Supervisory/Command	0.3092	0.0001

**19. It is legal to make multiple copies of a single software package without obtaining a site license as long as it is done for the Air Force's benefit on Air Force computers.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.2005	0.0149
Years of Military Ser.	-0.1884	0.0223
Have Used USAF Micro	-0.2029	0.0137
Frequency of Use	-0.2332	0.0045
Assigned a Micro	-0.1976	0.0165
Supervisory/Command	-0.2726	0.0008

20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1009	0.2225
Years of Military Ser.	-0.1873	0.0226
Have Used USAF Micro	-0.1661	0.0437
Frequency of Use	-0.1674	0.0421
Assigned a Micro	-0.1342	0.1039
Supervisory/Command	-0.1752	0.0332

21. It is ethical to make multiple copies of a single software package without a site license in order to save the Air Force money.

	CORRELATION	p-VALUE
Enlisted/Officer	-0.3147	0.0001
Years of Military Ser.	-0.1636	0.0470
Have Used USAF Micro	-0.1468	0.0750
Frequency of Use	-0.0878	0.2887
Assigned a Micro	-0.1297	0.1160
Supervisory/Command	-0.1885	0.0218

22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.

	CORRELATION	p-VALUE
Enlisted/Officer	0.1519	0.0654
Years of Military Ser.	0.1218	0.1403
Have Used USAF Micro	0.2529	0.0019
Frequency of Use	0.1593	0.0531
Assigned a Micro	0.1729	0.0356
Supervisory/Command	0.1316	0.1109

23. Software piracy does not occur on USAF microcomputers.

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1890	0.0214
Years of Military Ser.	-0.0816	0.3243
Have Used USAF Micro	-0.1743	0.0341
Frequency of Use	-0.1590	0.0535
Assigned a Micro	-0.1597	0.0526
Supervisory/Command	-0.2493	0.0023

**24. Under no circumstance would I use pirated software on an Air Force microcomputer.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1475	0.0757
Years of Military Ser.	0.1455	0.0797
Have Used USAF Micro	-0.0842	0.3126
Frequency of Use	-0.1444	0.0820
Assigned a Micro	-0.0446	0.5929
Supervisory/Command	-0.0660	0.4287

**25. I am not aware of any pirated software on USAF owned microcomputers.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1072	0.1963
Years of Military Ser.	0.0727	0.3814
Have Used USAF Micro	-0.1086	0.1906
Frequency of Use	-0.2223	0.0068
Assigned a Micro	-0.0922	0.2665
Supervisory/Command	-0.0677	0.4148

**26. Software piracy is a problem on Air Force micro-computers**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0041	0.9606
Years of Military Ser.	0.2227	0.0065
Have Used USAF Micro	0.0408	0.6222
Frequency of Use	0.1143	0.1666
Assigned a Micro	0.2149	0.0087
Supervisory/Command	0.2266	0.0056

**27. While I would not be involved with copying Air Force owned software, I personally have no problem with using pirated software on my home computer.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0742	0.5568
Years of Military Ser.	-0.0489	0.6992
Have Used USAF Micro	0.0475	0.7072
Frequency of Use	0.0851	0.5001
Assigned a Micro	-0.0376	0.7660
Supervisory/Command	-0.0102	0.9359

28. The availability of legally acquired software is adequate for my needs when using Air Force micro-computers.

	CORRELATION	p-VALUE
Enlisted/Officer	0.0052	0.9553
Years of Military Ser.	-0.0213	0.8175
Have Used USAF Micro	0.0594	0.5192
Frequency of Use	-0.0141	0.8788
Assigned a Micro	-0.1118	0.2242
Supervisory/Command	-0.0875	0.3422

29. At this time, the software on the computer(s) assigned to me for my use has all been obtained legally.

	CORRELATION	p-VALUE
Enlisted/Officer	0.0108	0.9192
Years of Military Ser.	-0.0018	0.9878
Have Used USAF Micro	-0.0018	0.9863
Frequency of Use	-0.0060	0.9556
Assigned a Micro	0.2085	0.0486
Supervisory/Command	0.1928	0.0687

30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0445	0.7166
Years of Military Ser.	-0.2288	0.0586
Have Used USAF Micro	-0.0317	0.7959
Frequency of Use	0.0355	0.7719
Assigned a Micro	-0.0890	0.4671
Supervisory/Command	-0.0897	0.4367

31. To the best of my knowledge, I have never used pirated software on Air Force microcomputers.

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0514	0.5742
Years of Military Ser.	0.0646	0.4797
Have Used USAF Micro	0.0237	0.7959
Frequency of Use	-0.0843	0.3560
Assigned a Micro	-0.0262	0.7743
Supervisory/Command	-0.0319	0.7269

**32. In the past, software piracy was justified on USAF computers.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1489	0.0709
Years of Military Ser.	-0.2132	0.0093
Have Used USAF Micro	-0/0995	0.2289
Frequency of Use	-0.0139	0.8667
Assigned a Micro	-0.1030	0.2130
Supervisory/Command	-0.1570	0.0567

**33. Today, I can find no justification for the Air Force or its members to violate the U.S. copyright law by unauthorized copying of commercial software.**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.0060	0.9419
Years of Military Ser.	0.1451	0.0784
Have Used USAF Micro	0.0073	0.9303
Frequency of Use	-0.1092	0.1865
Assigned a Micro	-0.0310	0.7082
Supervisory/Command	0.0620	0.4544

**34. Individuals involved with software piracy on USAF computers are not very likely to get caught.**

	CORRELATION	p-VALUE
Enlisted/Officer	0.1843	0.0250
Years of Military Ser.	-0.0898	0.2779
Have Used USAF Micro	0.0572	0.4901
Frequency of Use	0.0843	0.3087
Assigned a Micro	-0.0676	0.4143
Supervisory/Command	0.0152	0.8544

**35. Have you ever heard a superior condone unauthorized software copying?**

	CORRELATION	p-VALUE
Enlisted/Officer	-0.1267	0.1478
Years of Military Ser.	0.1592	0.0683
Have Used USAF Micro	0.1523	0.0813
Frequency of Use	0.1784	0.0407
Assigned a Micro	0.1294	0.1391
Supervisory/Command	0.2246	0.0098

36. Has anyone ever suggested that you make an unauthorized copy of copy protected software on a USAF micro-computer?

	CORRELATION	p-VALUE
Enlisted/Officer	0.0231	0.7929
Years of Military Ser.	0.1312	0.1336
Have Used USAF Micro	0.1569	0.0723
Frequency of Use	0.2446	0.0022
Assigned a Micro	0.2473	0.0043
Supervisory/Command	0.2067	0.0174

37. Due to circumstances beyond your control, have you ever knowingly used pirated software on an Air Force computer to accomplish your assigned duties?

	CORRELATION	p-VALUE
Enlisted/Officer	0.0296	0.7364
Years of Military Ser.	0.0721	0.4114
Have Used USAF Micro	0.1379	0.1148
Frequency of Use	0.2031	0.0195
Assigned a Micro	0.1381	0.1144
Supervisory/Command	0.1300	0.1374



Appendix F: Mean Survey Responses Along With  
p-Values for 2-Sample T-Test for Means  
Commander/Supervisor vs Non-Commander/Supervisor

**8. I understand the United States copyright law.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.23	3.61	0.0001

**9. I understand what software license agreements are.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.11	3.34	0.0001

**10. I know what software piracy is.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.48	3.96	0.0006

**11. The United States Air Force has formal regulations/policies covering illegal software copying by its members.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.39	4.04	0.0114

**12. My unit has formal regulations/policies covering illegal software copying by members of my unit.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.82	3.53	0.1132

**13. I understand what software can and cannot be used on an Air Force microcomputer.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.05	3.22	0.0000

**14. The Air Force aggressively tries to prevent illegal software copying on its microcomputers.**

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.23	3.27	0.8121

15. The Air Force is successful at preventing software piracy from occurring on its microcomputers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	2.39	2.83	0.0025

16. The Air Force actively inspects microcomputers to detect illegal software.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	2.80	3.02	0.1596

17. USAF microcomputer users are adequately informed about policies/regulations concerning software piracy.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.36	2.91	0.0165

18. I know the potential penalties for violating the U.S. copyright law on Air Force computers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.70	3.00	0.0001

19. It is legal to make multiple copies of a single software package without obtaining a site license as long as it is done for the Air Force's benefit on Air Force computers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	2.02	2.57	0.0008

20. It is legal to copy USAF purchased software onto my home computer if I am doing USAF related work on my home computer.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	2.05	2.39	0.0332

21. It is ethical to make multiple copies of a single software package without a site license in order to save the Air Force money.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	1.89	2.28	0.0218

22. It is as unethical to copy a \$300 copyrighted software package as it is to take \$300 worth of office supplies for personal use.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.14	3.83	0.1109

23. Software piracy does not occur on USAF microcomputers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	1.84	2.36	0.0023

24. Under no circumstance would I use pirated software on an Air Force microcomputer.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.65	3.81	0.4287

25. I am not aware of any pirated software on USAF owned microcomputers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.34	3.50	0.4148

26. Software piracy is a problem on Air Force microcomputers

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.52	3.12	0.0152

27. While I would not be involved with copying Air Force owned software, I personally have no problem with using pirated software on my home computer.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	2.88	2.90	0.9359

28. The availability of legally acquired software is adequate for my needs when using Air Force microcomputers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.60	3.80	0.3422

29. At this time, the software on the computer(s) assigned to me for my use has all been obtained legally.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.27	3.82	0.0687

30. As a commander/supervisor, I occasionally find it necessary for my subordinates to use pirated software to accomplish the mission.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	1.62	1.73	0.4637

31. To the best of my knowledge, I have never used pirated software on Air Force microcomputers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.66	3.74	0.7269

32. In the past, software piracy was justified on USAF computers.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	2.18	2.49	0.0567

33. Today, I can find no justification for the Air Force or its members to violate the U.S. copyright law by unauthorized copying of commercial software.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	4.00	3.88	0.4544

34. Individuals involved with software piracy on USAF computers are not very likely to get caught.

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	3.27	3.24	0.8544

35. Have you ever heard a superior condone unauthorized software copying?

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	1.73	1.91	0.0329

36. Has anyone ever suggested that you make an unauthorized copy of copy protected software on a USAF micro-computer?

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	1.73	1.89	0.0457

37. Due to circumstances beyond your control, have you ever knowingly used pirated software on an Air Force computer to accomplish your assigned duties?

	COM/SUP	NON-COM/SUP	p-VALUE
Mean	1.81	1.91	0.1949

#### Appendix G: Summary of Written Comments

1) One of our biggest problems is when other offices require data on a floppy using a program we don't legally own. The typical reaction is to "borrow" a copy of the software until we can legally obtain our own.

2) Software piracy is a big problem in the Air Force. Most of it is due to the lack of education. I work for a small computers customer service center and we work on computers all the time.

The other day, a captain and a Lt Col were asking why it isn't legal to copy Enable from a Z-248 to a Z-184 using an external floppy. We explained to them about the copyright laws, but they kept insisting that it's Fraud, Waste, and Abuse to have one copy for one computer and another for another computer somewhere else on base.

What the Air Force needs to do is set up computer training in tech training schools, etc. Teach them at the beginning and people will understand that it is illegal to pirate software.

3) It is really disturbing to me how people treat software like a magazine--passing it around and making copies if it interests them. I've seen people with xeroxed copies of the Lotus 1-2-3 manual, I mean we're talking 300+ pages! I'm

not sure if education is the answer, these people really believe that they're not hurting anyone or stealing anything

4) Don't know what you'll accomplish with this, but it won't help very much. If all you're after is numbers, then you'll do ok. But, if you're trying to stop the use of pirated software on A.F. computers, you might as well give up now, and save money. People will continue to use other software because they can. Not to make money, not to pin anyone off, but just 'cause they can. Oh well, good luck.

5) As of the time I left the Air Staff two years ago, using unauthorized copies of copy protected software was common. We tried to obtain enough legal copies to have word processing on all of our computers and data base management, spreadsheets, and graphics packages on selected computers. However, the software procurement process was not keeping up with the hardware procurement. Our action officers were under a lot of pressure to use their computers to keep up with the workload. They did what they had to do.

6) In the past, pirated software was used on occasion to accomplish mission (utility software to retrieve lost files) but adequate software is now legally owned. Funding at this base has been ample enough that illegal software is no longer needed or condoned.

7) I have used USAF microcomputers for about 4 years. During the first year there were programs that in retrospect probably were not authorized (i.e. purchased one copy and spread it to other computers; and also brought programs from home to work problems on USAF computers). We were briefed on what we could use and couldn't use IAW copyright laws. After that briefing (1985-86) we removed all unauthorized copies of programs, and purchased the ones we needed. In some cases we left unauthorized programs in computers but submitted paper work to buy the program (just didn't want to wait for the ok to process the system). (That was at HQ level). Now at Wg level we are very strict on what is on hard drives and disc files. If you have a program you had better have the documentation or evidence that it was purchased. Our wing small computer branch makes spot checks for unauthorized programs and reports findings to me. I think it was just a matter of education and follow up inspections. Folks don't want to intentionally violate copyright laws--red tape, regs, procedures, etc will not fix the problem...just tell folks what's correct/incorrect and why.

8) At my base, computer management drastically varies from organization to organization. Too often, computer/software violations are over looked. To date I have been through 4 inspections by off base teams, and not one has looked at one of my computers, other than to use my E-mail capability.



Education to the user level in the form of an interactive program taking no longer than 15 min at an eighth grade reading level, will at least inform the users. Enforcement has a cost and big brother can't watch everyone all the time.

9) Within my organization, monthly inspections are made to certify software loaded on PC's. Some PCs have games, various high level languages, and other unauthorized software loaded on them. Prior to inspections, this software is downloaded to floppys, so it is accessible for future use. Also, I know for a fact that a PC has an unauthorized copy of Turbo Pascal that is used by individuals pursuing degrees at a local university through off-duty education.

10) Although I do not know of any copyright law violations, I presume such problems are common. There is fairly little chance that my use of pirated material would be caught. One reason for this (I suspect) is that the only people capable of detecting and enforcing copyright infringements are those who have the greatest uses for the cheaper software.

11) The "system" makes it very difficult to obtain good software, in a timely manner, that is not on the "approved" software list. The "approved" software is generally difficult to learn and cumbersome to use, and I don't like being forced to use it! The "system" is so unresponsive, and

computers are so personal, that using unauthorized software, or pirating software to do the job is common.

12) The A.F. made a mistake by not standardizing in the beginning. Now there is so much garbage out there and fewer dollars to buy quality software--now that the A.F. has come closer to identifying what quality is.

13) I am currently assigned to a squadron that relies heavily on the use of microcomputers to accomplish its mission. I have heard of instances where software was unavailable and none could be purchased because ATC's spending level had been reached for small computers, so the only solution was to use an unauthorized copy to do the job. I don't think it's a problem over all, but I'm sure that there will always be cases where software is copied illegally.

14) The attitude with regard to copyright violation begins at the issuing station in my experience. When my Zenith lap top was issued, no mention was made about availability of programs, copyright protection, etc. The attitude was "here's your computer, good luck." Fortunately, most of the software I have needed was already loaded, thereby eliminating the temptation to seek other software, including my own home software.

15) Mission accomplishment is paramount.

16) I personally feel it's too hard to catch personnel using illegal material. Though it could eventually be found--the cost of finding material would exceed what's found.

17) I am a computer operator and have been around all kinds of minicomputers for the past 6 years. Problems--

- There are no methods of enforcement as far as piracy and illegal use of games etc. on USAF computers, therefore the compusec program as far as the area you are concerned about is very weak!! Lack of deterrent!!!

- The Air force wastes a lot of money when it has such a large variety of word processing software, wasted is time retraining (I've used 4 different programs, Wordstar, Peach-text, WordPerfect and Enable) Use of different WP programs in different shops and squadrons forcing reaccomplishment of work. Standardization is the name of the game, or so I've been told!!

18) Unfortunately due to funding constraints in the area of microcomputers, and the recent fiasco with contracts the obtaining of needed software on a timely basis is futile. Many times specific individual software packages make or break projects and tasks assigned. These situations will cause the user into a "piracy" atmosphere due to the criticality of the task at hand. Obtaining software under these

conditions becomes vital, and most personnel will opt to "borrow" what is needed rather than let taskings go uncompleted.

### Bibliography

1. Albrecht, Colonel Henry E., Director of Automation Support DCS/Command, Control, Communications, and Computer Systems. Personal Correspondence. HQ MAC/SCU, Scott AFB IL, 20 February 1990.
2. Athey, Susan. But I Didn't Know it was Wrong to Copy. Working Copy of Report. Colorado State University, Ft Collins CO, 1989.
3. ----- . "Software Copying Policies of the Fortune 500," Journal of Systems Management, 40: 31-35 (July 1989).
4. Beheshtian, M. "Computer Copyright Law," Journal of Systems Management, 37: 6-11 (September 1986).
5. Braue, Joseph. "Software Copying: Who's to Blame?," Computer Decisions, 17: 16-20 (26 February 1985).
6. Bray, Captain Anthony W., Chief, Resources Inspections Branch. Personal Correspondence. HQ SPACECOM/IG, Peterson AFB CO, 2 April 1990.
7. Bryant, S. F. "Software Thievery," Computer Decisions, 17: 42, 46 (15 January 1985).
8. Clevenger, Thomas B. and others. "Audit Opportunities to Control Software Piracy to Reduce Risk of Liability," Internal Auditor, 45: 42-47 (December 1988).
9. Cole, Brigadier General James L., Jr, Inspector General. Personal Correspondence. HQ MAC/IG, Scott AFB IL, 30 January 1990.
10. Cooper, F. L., III. Law and the Software Marketer. Englewood Cliffs NJ: Prentice Hall, 1988.
11. ----- and C. Sommerville. "Software Piracy: Is Your Company Liable?," The CPA Journal, unknown: 74-78 (March 1986).
12. Dauphinais, Lieutenant Paul Raymond. Copyright Law, Computer Software, and Government Acquisition. MS Thesis. Naval Postgraduate School, Monterey CA, September 1984 (AD-A150 347)

13. Department of the Air Force. Computer Security Policy. AFR 205-16. Washington: HQ USAF, 28 April 1989.
14. \_\_\_\_\_. Information Systems Security. AFR 700-10. Washington: HQ USAF, 15 March 1985.
15. \_\_\_\_\_. Inventions, Patents, Copyrights, and Trade-marks. AFR 110-8. Washington: HQ USAF, 28 July 1978.
16. \_\_\_\_\_. Management of Small Computers. AFR 700-26. Washington: HQ USAF, 15 December 1988.
17. \_\_\_\_\_. [Acquisition and] Management of Small Computers, AFCC Supplement 1. AFR 700-26. Scott AFB IL: HQ AFCC, 11 July 1986.
18. \_\_\_\_\_. Management of Small Computers, AFLC Supplement 1. AFR 700-26. Wright-Patterson AFB OH: HQ AFLC, 21 June 1988.
19. \_\_\_\_\_. Management of Small Computers, MAC Supplement 1. AFR 700-26. Scott AFB IL: HQ MAC, (draft).
20. \_\_\_\_\_. Management of Small Computers, PACAF Supplement 1. AFR 700-26. Hickam AFB HA: HQ PACAF, 4 May 1987.
21. \_\_\_\_\_. Management of Small Computers, SAC Supplement 1. AFR 700-26. Offutt AFB NE: HQ SAC, (draft).
22. \_\_\_\_\_. Management of Small Computers, SPACECOM Supplement 1. AFR 700-26. Peterson AFB CO: HQ SPACECOM, 22 July 1988.
23. Department of Defense. DoD FAR Supplement (DFAR). Chicago: Commerce Clearing House, Inc, 1988.
24. Federal Acquisition Regulation (FAR). Chicago: Commerce Clearing House, Inc, 1988.
25. Felton, Eric. "Hard Road to Software Copyright," Insight, 6: 54-55 (19 February 1990).
26. Gallegos, Frederick. "Personal Computer Application Software Protection," The EDP Auditor Journal, 1: 21-30 (1988).
27. Goodhue, Dale L. and Detmar W. Straub. "Security Concerns of System Users: A Proposed Study of User Perceptions of the Adequacy of Security Measures," Proceedings of the HICSS. 117-127. New York: IEEE Press, 1989.

28. Kalinowski, Colonel Sharon A., Deputy Inspector General for Inquiries, Review, and Oversight. Personal Correspondence. HQ AFSC/IGQ, Andrews AFB, Washington DC, 18 January 1990.
29. Kundert, Thomas, Chief, Patent Prosecution Office. Telephone conversation. AF/JACPD, Wright-Patterson AFB OH, 16 May 90.
30. Lewenstein, Bruce V. "The Ethics of Software Piracy," PC Magazine, 4: 179, 182+ (April 1985).
31. McMahon, Gene. "Putting a Lid on Software Piracy," Corporate Law, unknown: 57-59 (June 1984).
32. McMillan, Colonel Victor R., Acting Director, Arch, Policy & Tech ACS/Systems for Command, Control, Communications and Computers. Personal Correspondence. HQ USAF/SCT, Washington DC, 30 Jan 1990.
33. Mason, Janet. "Crackdown on Software Pirates, Industry Watchdogs Renew Efforts to Curb Illegal Copying," Computerworld, 24: 107+ (5 February 1990).
34. Micossi, A. "Software Piracy 'Shrinks' by 90%," Computer Decisions, 17: 28 (2 July 1985).
35. "Novell Wins Damages in Copyright Dispute," Deseret News, 40: unknown (28 December 1989).
36. Ranney, Elizabeth. "Piracy Problem Plagues Corporate Managers," InfoWorld, 7: 1,8 (2 September 1985).
37. Scott, Michael D. Computer Law. New York: Wiley Law Publications, 1984.
38. Shim J.P. and G. Stephen Taylor. "Business Faculty Members' Perceptions of Unauthorized Software Copying," OR/MS Today, 15: 30-31 (October 1988).
39. -----. "Practicing Managers' Perception/Attitudes Toward Illegal Software Copying," OR/MS Today, 16: 30-33 (August 1989).
40. Shine, Captain Michael A., Chief, Small Computer Tech Center, Directorate of Operations. Personal Correspondence. HQ SAC, Offutt AFB NE, 25 January 1990.
41. Solomon, Susan L. and James A. O'Brien. The Effect of Demographic factors on Attitudes Toward Software Piracy. Unpublished Report. California State University, Sacramento CA (date unknown).

42. Straub, Detmar W. and Rosann Webb Collins. "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," MIS Quarterly, 14: 45-46 (June 1990).
43. Thou Shalt Not Dupe. ADAPSO, Arlington VA, 1984.
44. Uniform Code of Military Justice. Washington: United States Government Printing Office, date unknown.
45. United States Congress. Title 17, United States Code. St Paul MN: West Publishing Co, 1987.
46. -----. Title 17, United States Code, 1989 Cumulative Annual Pocket Part. St Paul MN: West Publishing Co, 1989.
47. -----. Title 28, United States Code. St Paul MN: West Publishing Co, 1970.
48. United States, National Commission on New Technological Uses of Copyrighted Works. Final Report of the National Commission on New Technological Uses of Copyrighted Works, June 13, 1978. Washington: Library of Congress, 1979.
49. VMS SAS Production Release 6.02. Cary NC: SAS Institute, Inc.
50. Wybo, Michael D. and Detmar W. Straub, Jr. "Protecting Organizational Information Resources," Information Resources Management Journal, 2: 1-15 (Fall 1989).



Vita

First Lieutenant Jay Chris Sorensen [REDACTED]

[REDACTED] He graduated from Hillcrest High School in Midvale, Utah in 1977 and attended Brigham Young University and Utah State University, graduating with a Bachelor of Science in Range Science (specialty: Range Management) in June 1984. After working as a state lands manager in Utah and New Mexico he attended Officer Training School at San Antonio, Texas. Upon graduating in June 1987, he served his first tour of duty at Eglin AFB, Florida as an executive officer to the commander of the 3246th Organizational Maintenance Squadron. His tour at Eglin was made short when he was selected for the Air Force Institute of Technology as a second lieutenant. He entered the School of Systems and Logistics in the Information Resource Management program in May 1989.

[REDACTED]  
Permanent Address: [REDACTED]  
[REDACTED]

# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 1990		3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE UNITED STATES COPYRIGHT LAW AND SOFTWARE PIRACY ON UNITED STATES AIR FORCE MICROCOMPUTERS				5. FUNDING NUMBERS	
6. AUTHOR(S) Jay C. Sorensen, 1st Lieutenant, USAF					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology, WPAFB OH 45433-6583				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/GIR/LSY/90D-11	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES					
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited				12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) This study looked at the United States Copyright Law and its applications to computer software. The study looked at USAF policies and regulations governing the protection of copyrighted software. The literature review, including personal correspondence with inspector generals and computer and legal personnel, indicated that the Air Force has numerous policies concerning software copyright and the violation of those copyrights (software piracy). These policies and regulations were compared to standards set by the software industry and the results suggested that the appropriate policies are in place, but in some instances, enforcement was lacking. An attitudinal survey was conducted with 125 enlisted personnel and 125 officers, with a 58.4 and 60.0 percent usable return rate. Using a simple 5-point Likert scale and "Yes/No" questions, no overall significant differences of attitudes were demonstrated between the two populations. While many of the respondents felt that there was a problem with software piracy, few claimed to be personally involved. Understanding of copyright laws and what can and cannot be legally copied on micro-computers was lacking, especially in the junior ranks. Overall, it was determined that entry level education and enforcement of policies governing software piracy need to be increased.					
14. SUBJECT TERMS Copyrights, Computer Programs, Microcomputers, Ethics, Patents				15. NUMBER OF PAGES 161	
				16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL		